|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Information Security Program Policy | | | | | |
| Policy # | CPL-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](#_Toc457885274)

[Scope 1](#_Toc457885275)

[Policy 1](#_Toc457885276)

[Programs 1](#_Toc457885277)

[Policy and Procedures Requirements 2](#_Toc457885278)

[Policy Sanctions 2](#_Toc457885279)

[Policy Exceptions 2](#_Toc457885280)

[Policy Distribution 2](#_Toc457885281)

[Policy Review 3](#_Toc457885282)

[Responsibility Assignment 3](#_Toc457885283)

[Program Reporting 3](#_Toc457885284)

[Program Review and Maintenance 4](#_Toc457885285)

[Security in Project Management 4](#_Toc457885286)

[Security Program Compliance 4](#_Toc457885287)

[Violations 4](#_Toc457885288)

[Definitions 4](#_Toc457885289)

[References 5](#_Toc457885290)

[Related Documents 5](#_Toc457885291)

[Approval and Ownership 5](#_Toc457885292)

[Revision History 5](#_Toc457885293)

Purpose

This policy establishes the minimum requirements and responsibilities for the protection of Company X information assets, preventing the misuse and loss of information assets, establishing the basis for audits and self-assessments, and preserving Company X management options and legal remedies in the event of asset loss or misuse.

Scope

This policy applies to all Company X computer systems and facilities, including those managed for Company X by third-parties. This policy applies to all employees, partners and third-parties with access to Company X information assets.

Policy

### Programs

Information Security Program - Company X must implement a comprehensive, written information security program that will secure Company X information assets in a manner commensurate with each asset’s value as established by risk assessment and mitigation measures.

Information Privacy Program - Company X must implement a comprehensive, written information privacy program that will secure Company X employee and customer personally identifiable information (PII) against unauthorized use or disclosure.

### Policy and Procedures Requirements

Information Asset Security Policies - Policies must be implemented and enforced to assure the security, reliability, integrity, and availability of Company X information assets.

Information Asset Security **Procedures** - Procedures must be implemented and enforced to enforce security policies and assure the security, reliability, integrity, and availability of Company X information assets.

Accidental or unauthorized events - Policies must be implemented and enforced to protect Company X information assets against accidental or unauthorized modification, disclosure, or destruction.

### **Policy Sanctions**

Policy Sanctions – Company X must implement sanctions against employees and third parties who violate the written policies.

Policy Sanction Disciplinary Process - Assuming the action is inadvertent or accidental, first violations of information security policies or procedures must result in a warning. Second violations involving the same matter must result in a letter being placed in the involved worker's personnel file. Third violations involving the same matter must result in a five-day suspension without pay. Fourth violations involving the same must result in dismissal. Willful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including immediate dismissal.

### Policy Exceptions

**Documented Policy Exception Process -** Company X must maintain a documented process for tracking and approving exceptions to information security policies and procedures.

**Exceptions to Policies -** All Company X employees responsible for information security must submit a written request for exceptions to conform to information security policies. Such exceptions must be approved by a member of the information security department and the internal audit department.

**Periodic Review of Documented Policy Exceptions —** All documented and approved exceptions to Company X security policy must be reviewed at least every six months.

### Policy Distribution

**Security Policy Document Distribution -** Company X management must publish written information security policies and make them available to all employees and relevant external parties.

**Acknowledgement of Security Policies —** All Company X employees and contractors must review and acknowledge acceptance of the information security policies which apply to them at least on an annual basis.

**Policy Document Classification –** All Company X security policy documents must be labeled as CONFIDENTIAL – Internal Use Only and revealed only to Company X workers and selected outsiders (such as auditors) who have a legitimate business need for this information.

### Policy Review

**Annual Review of Information Security Policy Documents** - All Company X written information security policy documents must be reviewed on an annual basis by a team consisting (at a minimum) of members from the information security, legal and human resources departments.

**Policy Document History** – Management must keep a history of previous versions of information security policies, standards and procedures for a period of seven years.

### Responsibility Assignment

**Information Security Resources** - Management must allocate sufficient resources and staff attention to adequately address information systems security.

**Defining Specific Security Roles** – Company X must define specific job roles required for the effective implementation of the Company X information security program. Each role must include a specific description of the information security-related duties performed by each team member performing those job functions.

**Management Responsibility and Accountability -** Information security is a management responsibility, and decision-making for information security must not be delegated. While specialists and advisors play an important role in helping to make sure that controls are designed properly, functioning properly, and adhered to consistently, it is the manager in charge of the business area involved who is primarily responsible for information security.

**Assigning Security Officer** – Company X must explicitly define at least one individual responsible for the duties of the information security function. This role will be entitled “Information Security Manager.”

**Clear Assignment of Control Accountability -** Company X management must clearly assign and document accountability for every internal control at Company X. This accountability must include sufficient transparency so that top management will be kept informed about the effectiveness and efficiency of these same internal controls.

### **Program Reporting**

**Annual Security Program Report** - Annual reports must be submitted to Company X management that includes information on:

* The status of the program
* The updated risk assessment and analysis.
* Management decisions for the level of risk mitigation and residual risk accepted.
* Service provider oversight activities and status.
* The results of testing of key controls.
* Management's response to any identified deficiencies and recommendations for program changes.
* The independent validation of the information contained in the report.

### Program Review and Maintenance

**Annual Program Updates** - The information security program must be updated and re-approved by Company X management annually or whenever there is a material change in the organization or infrastructure.

**Risk Assessments** - The information security program must be updated, as appropriate, based on the results of the organization's risk assessment and any risk assessment completed by a third party.

### Security in Project Management

**Information Security Impact Analysis** - Whenever a new system or project involves sensitive information, the Information Security Manager must ensure that information security considerations are part of the project management and review process. For example, new systems must have information security requirements identified up front.

### Security Program Compliance

**Laws, Regulations And Contractual Requirements** – The control requirements for the Company X information security program must include an analysis and definition of all relevant statutory, regulatory, and contractual requirements.

**Information System Control Reviews — Independent** - An independent and externally-provided review of information systems security must be periodically obtained to determine both the adequacy of and compliance with controls.

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.

Any employee or partner 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 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.

**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.

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

References

CPL: 3.0 – Security Program Management

ISO 27002: 5.1 Management direction for information security

HIPAA: Security Management Process 164.308(a)(1)

NIST: PL-1 Security Planning Policy and Procedures

PCI: R12. Maintain a security policy for all personnel

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 |  |
|  |  |  |  |  |