|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| IT Risk Management Policy | | | | | |
| Policy # | CPL-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888.641.0500 |

**Table of Content**

[Purpose 1](#_Toc444589140)

[Scope 1](#_Toc444589141)

[Policy 1](#_Toc444589142)

[IT Risk Management Process 1](#_Toc444589143)

[Risk Treatment 2](#_Toc444589144)

[Information Systems Risk Management 2](#_Toc444589145)

[Insurance 2](#_Toc444589146)

[Violations 2](#_Toc444589147)

[Definitions 2](#_Toc444589148)

[References 3](#_Toc444589149)

[Approval and Ownership 3](#_Toc444589150)

Purpose

This policy defines the requirements for reporting and responding to incidents related to Company X information assets and systems.

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

### ****IT Risk Management Process****

**Enterprise Security Risk Assessment -** Each year Information Technology (IT) must conduct, or manage an independent party who conducts, an organization-wide security risk assessment. **The report resulting from this project must include a detailed description of the information security risks currently facing the organization, and specific recommendations for preventing or mitigating these risks.**

**Annual Information Technology Risk Report** - For the Board of Directors to properly perform its risk management role, IT management must submit to the Board a special annual report. This report is to include a description of all material Company X information technology-related risks, as well as an assessment of how these risks are currently being managed.

**Risk Assessment Methodology** – To create consistent results, Company X must adopt and document a formal risk assessment process be used where specified by Corporate Information Assurance\Security policies, or by laws or regulations. (For example, Company X risk assessments are to be conducted using the Facilitated Risk Assessment process (FRA). (cf. *Risk Management Guide for Information Technology Systems*, NIST SP 800-30.)

### Risk Treatment

**Material\Significant Information Security Risks** - For every material\significant information systems security risk identified -- whether through a formal risk assessment or not -- management must make a specific decision about the degree to which Company X will be self-insured and accept the risk, seek external insurance, or adjust controls to reduce expected losses to an acceptable cost of conducting business.

**Internal Controls Responsibility** – Every information security-related control identified within the Company X environment must be specifically assigned to responsible individual or team.

### Information Systems Risk Management

**Information Security Impact Analysis - Whenever sensitive information is to be placed in computers or whenever sensitive information is to be used in new or substantially different ways on computer systems, a risk assessment of the potential security-related impacts must be performed.**

### ****Insurance****

**Insurance Coverage** - Company X will maintain insurance commensurate with those residual risks identified from a corporate Risk Assessment or BIA which pose potential for financial loss or other disastrous consequences, as well as the expenses related to recovering from a disaster.

**Insurance Review** - The CFO will conduct an annual insurance review to ensure that the level and types of coverage are commercially reasonable and consistent with any legal, management, and board requirements.

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 willful and deliberate conduct that is 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

**Availability** - The state that exists when information resources are accessible and usable upon demand by an authorized user.

**Confidentiality** - The state that exists when data is held in confidence and is protected from unauthorized disclosure to unauthorized individuals, entities, or processes. Misuse of data beyond the scope of their duties by those authorized to use it is also considered to be a violation of data confidentiality.

**Control** - Security mechanisms implemented to prevent, detect, reduce or eliminate risks. In doing so, controls maintain the properties of **availability, integrity,** and **confidentiality**.

**Integrity** - The state that exists when data is the same as that in the source documents, or has been correctly computed from source data, and has not been exposed to accidental alteration or destruction. Incomplete data, unauthorized changes, or additions to the data, and erroneous source data are all considered violation of data integrity.

**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.

**Risk** - The result of a threat acting on a vulnerability, expressed as a product of likelihood (probability) and severity (of impact.)

**Risk Assessment** - The determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat or hazard. The result of a risk assessment is typically a report that shows assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.

**Residual Risk** – The risk that remains after a control is applied to an identified risk, and that control does not eliminate the risk.

**Risk Cost\Benefit\Impact Evaluation** – The process of evaluating risk compared to value of information-related assets and amount of damage done to system or owner should the system or data be compromised or damaged.

**Risk Mitigation** – The process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process.

**Facilitated Risk Assessment** – This process, which utilizes a “qualitative” risk analysis, is geared to a specific application, system or network. It allows risks to be addressed in financial and non-financial terms, as well as taking into consideration secondary impacts. It is a formal methodology that is driven by the system’s owners, conducted by a facilitator, and can be completed in a relatively short period of time.

**Threat** - Any person, object or event that, if realized, could potentially cause damage to an information resource or the data processed on those resources. This includes damage to the **availability, integrity**, and/or **confidentiality** of resources or information.

**Vulnerability** - Weaknesses in an information resource that can be exploited by a threat.

References

ISO/IEC 27002: 4.0 Risk Management

CPL: 1.0 - IT Risk Management

NIST: Risk Assessment (RA)

NIST SP 800-30 – Risk Assessment Guide

PCI-DSS: 12.2 Annual Risk Assessments

HIPAA: Security Management Process - Risk Management (R)

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 |  |
|  |  |  |  |  |