*IT Risk Management Policy*

**Table of Contents**

[Purpose 1](#_Toc2682811)

[Scope 1](#_Toc2682812)

[Policy 1](#_Toc2682813)

[Risk Management Process 1](#_Toc2682814)

[Information Systems Risk Management 2](#_Toc2682815)

[Risk Treatment - Controls 2](#_Toc2682816)

[Risk Treatment - Insurance 2](#_Toc2682817)

[Violations 3](#_Toc2682818)

[Definitions 3](#_Toc2682819)

[References 4](#_Toc2682820)

[Related Documents 4](#_Toc2682821)

[Approval and Ownership 4](#_Toc2682822)

[Revision History 5](#_Toc2682823)

Purpose

This policy defines the requirements for the identification of information security risks and the appropriate control posture required to reduce risk for all CompanyX (the “Company”) information system assets.

Scope

This policy applies to all CompanyX information assets, systems and facilities, with a target audience of CompanyX Executive Management, Information Technology employees and Third-Parties responsible for information security risk management.

Policy

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

**Enterprise Security Risk Assessment -** Each year the Information Security Department in conjunction with 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.**

**Business Unit Risk Assessment** - Each critical organizational or business unit within CompanyX that manages its own computers or networks must also perform, at least annually, a security-related risk analysis of these same systems, coordinated through the Information Security Department, and then certify that adequate security measures have been implemented to mitigate the 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 CompanyX information technology-related risks, as well as an assessment of how these risks are currently being managed.

**Risk Assessment Methodology** – To create consistent results, CompanyX 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, CompanyX 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.)

### 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 Information systems, a risk assessment of the potential security-related impacts must be performed.**

**Production System Risk Assessments - Information systems security risk assessments for critical information systems and critical production applications must be performed at least once every two years. All major enhancements, upgrades, conversions, and related changes associated with these systems or applications must be preceded by a risk assessment.**

### Risk Treatment - Controls

**Control Framework** – CompanyX will adopt and information security control framework designed to mitigate information security risks and comply with regulatory and contract requirements for information security.

**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 CompanyX 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.

**Control Responsibility Assignment** – CompanyX management must specifically assign responsibility for the control measures protecting every major information asset.

### ****Risk Treatment - Insurance****

**Insurance Coverage** - Adequate insurance coverage must be obtained and kept in force for every major threat facing the confidentiality, integrity, and availability of information handled by CompanyX Information systems.

**BCP and Insurance** - CompanyX will maintain insurance commensurate with those residual risks identified from a corporate 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.

**BCP System Inventory** - To facilitate the insurance claims process, the IT Continuity Planning Team will create and retain a comprehensive hardware and software inventory list and the Business Continuity Planning Team will create a comprehensive business asset inventory list.  Copies of both inventories are to be retained in a secure off-site location along with copies of all other Continuity Planning documentation.  A detailed accounting of expenses incurred during recovery or restoration should be documented to support insurance claims.

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-Party 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

**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 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.

**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 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.

References

ISO/IEC 27002: 4.0 Risk Management

NIST: Risk Assessment (RA)

NIST SP 800-30 – Risk Assessment Guide

PCI-DSS: 12.2 Annual Risk Assessments

US-CSF: ID.RA: Risk Assessment

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 |  |
|  |  |  |  |  |