Information Security Policy

Sample Organization

Criteria satisfaction

Standard	Criteria Satisfied
TSC 2017	CC9.9

Document history

Date	Comment
Jun 1 2018	Initial document

Contents

1 Purpose and Scope

a. This information security policy defines the purpose, principles, objectives and basic rules for information security management.

b. This document also defines procedures to implement high level information security protections within the organization, including definitions, procedures, responsibilities and performance measures (metrics and reporting mechanisms).

c. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily available to all users.

2 Background

a. This policy defines the high level objectives and implementation instructions for the organization's information security program. It includes the organization's information security objectives and requirements; such objectives and requirements are to be referenced when setting detailed information security policy for other areas of the organization. This policy also defines management roles and responsibilities for the organization's Information Security Management System (ISMS). Finally, this policy references all security controls implemented within the organization.

b. Within this document, the following definitions apply:

   i. *Confidentiality*: a characteristic of information or information systems in which such information or systems are only available to authorized entities.

   ii. *Integrity*: a characteristic of information or information systems in which such information or systems may only be changed by authorized entities, and in an approved manner.

   iii. *Availability*: a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed.

   iv. *Information Security*: the act of preserving the confidentiality, integrity, and, availability of information and information systems.

   v. *Information Security Management System (ISMS)*: the overall management process that includes the planning, implementation, maintenance, review, and, improvement of information security.

3 References

a. Encryption Policy

b. Data Center Security Policy

c. Disaster Recovery Policy

d. Password Policy

e. Remote Access Policy

f. Removable Media/Cloud Storage/BYOD Policy

g. Risk Assessment Policy

h. Security Incident Response Policy

i. Software Development Lifecycle Policy

j. System Availability Policy

k. Workstation Security Policy

4 Policy

a. *Managing Information Security*

i. The organization's main objectives for information security include the following:

1. [list the reasons/objectives for maintaining information security at the organization. Examples include a better market image, reduced risk of data breaches and compromises, and compliance with legal, regulatory, and contractual requirements.]

ii. The organization's objectives for information security are in line with the organization's business objectives, strategy, and plans.

iii. Objectives for individual security controls or groups of controls are proposed by the company management team, including but not limited to [list key roles inside the organization that will participate in information security matters], and others as appointed by the CEO; these security controls are approved by the CEO in accordance with the Risk Assessment Policy (Reference (a)).

iv. All objectives must be reviewed at least once per year.

v. The company will measure the fulfillment of all objectives. The measurement will be performed at least once per year. The results must be analyzed, evaluated, and reported to the management team.

b. *Information Security Requirements*

i. This policy and the entire information security program must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to the organization.

ii. All employees, contractors, and other individuals subject to the organization's information security policy must read and acknowledge all information security policies.

iii. The process of selecting information security controls and safeguards for the organization is defined in Reference (a).

iv. The organization prescribes guidelines for remote workers as part of the Remote Access Policy (reference (b)).

v. To counter the risk of unauthorized access, the organization maintains a Data Center Security Policy (reference (c)).

vi. Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Software Development Lifecycle Policy (reference (d)).

vii. Security requirements for handling information security incidents are defined in the Security Incident Response Policy (reference (e)).

viii. Disaster recovery and business continuity management policy is defined in the Disaster Recovery Policy (reference (f)).

ix. Requirements for information system availability and redundancy are defined in the System Availability Policy (reference (g)).