Information Systems and Technology Security Policy

Original author's name:	Pkkirisankar Jagannath
Most recent date:	November 22, 2022
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	November 22, 2022	Pkkirisankar Jagannath	Original Draft
v1.0	November 22, 2022	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	November 22, 2023

Information Systems and Technology Security Policy

As stated in the Company's Information Security Program Charter, the Company will follow a risk management approach to develop and implement information security policies, standards, guidelines, and procedures. The information security program will protect information assets by establishing policies to identify, classify, and define protection and management objectives, and define acceptable use of Company information assets.

This Information Systems and Technology Security Policy define Company objectives for establishing specific standards on the protection of the confidentiality, integrity, and availability of Company information assets.

1. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises, at hosted or outsourced sites, or who have been granted access to Company information or systems, are covered by this policy and must comply with associated standards and procedures unless an exception has been granted by the CEO.

The Company **Information Security Program Charter** and relevant policies, standards and guidelines must have the fundamental guidance, procedures, and commentary based upon the ISO 27001.

The ISO 27001 standard is a code of practice for information security subject to the guidance provided within ISO 27001.

The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices.

2. Objectives

The information security objectives from a holistic perspective that must be addressed in the subordinate control documents; standards, procedures, and supporting documentation are described as follows.

a. **Asset Identification and Classification**

The Asset Identification and Classification standards define Company objectives for establishing specific standards on the identification, classification, and labeling of Company information assets.

b. **Asset Protection**

The Asset Protection standards define the Company objectives for establishing specific standards on the protection of the confidentiality, integrity, and availability of Company information assets.

c. **Asset Management**

The Asset Management standards define Company objectives for establishing specific standards for the management of the networks, systems, and applications that store, process and transmit Company information assets.

d. **Acceptable Use**

The Acceptable Use standards define Company objectives for establishing specific standards on appropriate business use of the Company's information and telecommunications systems and equipment.

e. **Vulnerability Assessment and Management**

The Vulnerability Assessment and Management standards define the Company's objectives for establishing specific standards for the assessment and ongoing management of vulnerabilities.

f. **Threat Assessment and Monitoring**

The Threat Assessment and Monitoring standards define Company objectives for establishing specific standards for the assessment and ongoing monitoring of threats to Company information assets.

g. **Security Awareness**

The Security Awareness standards define Company objectives for establishing a formal Security Awareness Program, and specific standards for the education and communication of the Information Security Program Charter and associated policies, standards, guidelines, and procedures.

3. Responsibilities

The Company Technology Steering Committee is the approving authority for the Information Systems and Technology Security Policy.

The CEO is responsible for the development, implementation, and maintenance of the Information Systems and Technology Security Policy and associated standards and procedures while the CEO authorizes the approval of the Information Systems and Technology Security Policy, standards, and associated procedures.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using Company information assets:

Owners, as cited within the system of record are managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CEO will make the designation. Owners are responsible for defining procedures that are consistent with the intent defined by the Information Systems and Technology Security Policy and associated standards, ensuring the confidentiality, integrity and availability of information assets; authorizing access to those who have an approved business need for the information; and ensuring the revocation of access for those who no longer have a business need for the information.

Custodians are the managers, administrators, and those designated by the Owner to manage, process, or store information assets. Custodians are responsible for providing a secure processing environment that protects the confidentiality, integrity and availability of information; administering access to information as authorized by the Owner; and implementing procedural safeguards and cost-effective controls.

Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for using the information only for its intended purposes, and for maintaining the confidentiality, integrity and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

4. Policy Enforcement and Exception Handling

Failure to comply with the Information Systems and Technology Security Policy and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Information Systems and Technology Security Policy should be submitted to the CEO. Exceptions shall be permitted only on receipt of written approval from the CEO. The CEO will periodically report to the Company Board of Directors or designated committee concerning the current status of policy and standard implementations.

5. Review and Revision

The Information Systems and Technology Security Policy will be reviewed and revised in accordance with the **Information Security Program Charter**.

Recommended: ______________________

Signature

Pakkirisankar Jagannath

Program Manager

Approved: __________________________

Signature

Anil Sharma

CEO