Information Systems and Technology Security

Asset Protection Standard

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

Asset Protection Standard

As stated in the Company **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 Asset Protection Standard defines Company objectives for establishing specific standards on the protection of the confidentiality, integrity, and availability of Company information assets. Company information assets are defined in the **Asset Identification and Classification Standard**.

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 guidelines.

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

Authorization for access to information assets will be based on the classification of the information and defined to provide only the level of access required to meet an approved business need or perform prescribed job responsibilities.

Proper identification and authentication are required. Specific instructions and requirements for controlling access to information assets are provided in the **Access Control Standard**.

Authorization for remote access to information assets will be provided only to meet an approved business need or perform prescribed job responsibilities. Remote access must be facilitated by using Company-approved methods and programs. Specific instructions and requirements for accessing information assets remotely are provided in the **Remote Access Standard**.

Information assets must be protected with physical access control of areas containing information assets or processing activities. The physical access controls must be commensurate with the classification of the information and defined to provide only the level of physical access required to meet an approved need or perform prescribed job responsibilities. Specific instructions and requirements for physical access to information assets are provided in the **Physical Access Standard**.

The supporting infrastructure for systems, networks, telephony, and hardware should be protected from failure and regularly inspected or tested, as appropriate. Supporting infrastructure includes electricity or other power sources, water supply, cabling, external communication lines, heating and air conditioning equipment, sewage, etc.

Encryption must be used to protect Restricted and Confidential information assets that will be transmitted over non-secure or public networks. Storage of Restricted and Confidential information assets must be achieved with similar approved encryption methods. Only Company-approved encryption algorithms and products can be used to protect Restricted and Confidential information. Specific instructions and requirements for encryption are provided in the **Encryption Standard**.

Information assets must be created and maintained with appropriate controls to ensure that the information is correct, auditable, and reproducible. Specific instructions and requirements for protecting the integrity of information assets are provided in the **Integrity Protection Standard**.

The Company must establish appropriate controls to ensure information assets are consistently available to conduct business. Business continuity planning to effectively back up, replicate, and recover information assets, as necessary, must be established. Specific instructions and requirements for protecting the availability of information assets are provided in the **Availability Protection Standard**.

Information assets must be protected from destructive software elements such as viruses and malicious code that impair normal operations. Company-approved virus detection programs must be installed, enabled, and updated on all systems susceptible to viruses and malicious code. Specific instructions and requirements for protecting information assets from viruses and malicious code are provided in the **Anti-Virus Standard**.

Auditing must be activated to record relevant security events. The audit logs must be securely maintained for a reasonable period of time. Specific instructions and requirements for auditing information assets are provided in the **Auditing Standard**.

3. Responsibilities

The **CEO** is the approval authority for the Asset Protection Standard.

The **Program Manager** is responsible for the development, implementation, and maintenance of the Asset Protection Standard and associated standards and guidelines.

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 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 Asset Protection Standard 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 Asset Protection Standard 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 Asset Protection Standard should be submitted to the Program Manager. Exceptions shall be permitted only on receipt of written approval from the Program Manager. The Program Manager will periodically report current status to the CEO or its designee.

5. Review and Revision

The Asset Protection Standard will be reviewed and revised in accordance with the **Information Security Program Charter**.

Recommended: _____

Signature

Pakkirisankar Jagannath

Program Manager

Approved: _____

Signature

Anil Sharma

CEO