Information Systems and Technology Security

Asset Identification and Classification 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 Identification and Classification Standard

As stated in the **22nd Century Technologies** (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, define protection and management objectives, and define acceptable use of Company information assets.

This Asset Identification and Classification Standard define Company objectives for establishing specific standards on the identification, classification, and labeling 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 supporting the Company, or who have been granted access to Company information or systems, are covered by this standard 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.

An **information asset** is defined as any data, or an aggregate of data, that has value to the organization. This includes all data, whether in the form of electronic media or physical records that are used by the Company or in support of Company business processes, including all data maintained or accessed through systems owned or administered by or on the behalf of the Company. Information assets include all personal, private, or financial data about employees, clients, contractors, or other organizations that must be

protected in accordance with relevant legislative, regulatory, or contractual requirements.

2. Objectives

The Company defines information classifications based on the sensitivity, criticality, confidentiality/privacy requirements, and value of the information. All information assets, whether generated internally or externally, must be categorized into one of these information classifications: Restricted, Confidential, Internal Use Only, or Public. When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources. Specific instructions and requirements for classifying information assets are provided in the **Information Classification Standard and** specific instructions and requirements for labeling information assets are provided in the **Information Labeling Standard**.

3. Responsibilities

The CEO is the approval authority for the Asset Identification and Classification Standard.

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

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

- **Owners** are managers of organizational units listed in the system of record 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 identifying information assets; assigning the proper information classification; ensuring the proper handling of sensitive information; designating the Custodian in possession of the information; ensuring the information classifications are properly communicated and understood by the

Custodians; and reviewing information assets periodically to determine if their classifications should be changed.

- **Custodians** are the managers, administrators, service providers, and those designated by the Owner to manage, process, or store information assets. Custodians are responsible for understanding the information classifications, and applying the necessary controls (specified in the **Asset Protection Standard**) to maintain and conserve the information classifications and labeling established by the Owners.
- **Users** are the individuals, groups, or organizations authorized to access information assets. Users are responsible for understanding the information classifications, abiding by the controls defined as well as maintaining and preserving the information classification and labeling established by the Owners.

4. Enforcement and Exception Handling

Failure to comply with the Asset Identification and Classification 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 Identification and Classification 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 Identification and Classification 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