Information Systems and Technology Security

Information 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

Copyright © November 22, 2022 22nd Century Technologies

All rights reserved. This document is for internal use only. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the expressed written permission of 22nd Century Technologies.

Information Classification Standard

The **22nd Century Technologies** (the "Company") **Asset Identification and Classification Policy** define objectives for establishing specific standards on the identification, classification, and labeling of Company information assets.

This Information Classification Standard builds on the objectives established in the **Asset Identification and Classification Policy**, and provides specific instructions and requirements for classifying information assets. These instructions include Confidentiality, Integrity, Availability information classification requirement as well as reclassification and declassification requirements.

1. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or who have been granted access to Company information or systems, are covered by this standard and must comply with associated guidelines and procedures.

- **Availability** refers to ensuring the availability of information assets.
- **Confidentiality** refers to protecting sensitive information assets, including data related to privacy.
- **Configuration Management** refers to a collection of related processes pertaining to systems configuration that include functions such as hardware and software tracking; standard configurations and computing environments; and periodic auditing and compliance checking.
- **Information assets** are defined in the **Asset Identification and Classification Standard**.
- **Integrity** refers to ensuring the audit-ability and reproducibility of information assets.
- **Protection standard** refers to the required security configuration for a network device or system.
- **System Development Life Cycle** refers to the process of securely developing systems through several sequential phases, including requirement analysis, architecture and design, development, testing, deployment, operations/maintenance, and retirement.

2. Requirements

A. Confidentiality

All Company information shall be classified in one of four confidentiality categories:

- **Restricted**
- **Confidential**
- **Internal Use Only**
- **Public**

A description of each category is provided in the following table:

Confidentiality Classification	Description	Examples
Restricted	Information, the unauthorized disclosure of which would: Proprietary Information, Research Data protected by state and/or federal regulations	Examples may include: Potential criminal charges and/or massive legal fines or cause irreparable damage to company
Confidential	Information, the unauthorized disclosure of which would: PII, CUI, SBU, or other sensitive but non-classified data	Examples may include: Potential criminal charges and/or massive legal fines or cause irreparable damage to company
Internal Use Only	Information confined to use only within Company for purposes related to its business.	Examples may include: Data that has been classified as being for official or internal use only, such as work logs
Public	Information and material to which access may be granted to any other person or organization.	Examples may include: data that has been approved for public release, press release data

When **Restricted** information is combined with Confidential, Internal Use Only or Public information, the resulting collection of information must be classified as Restricted.

When **Confidential** information is combined with Internal Use Only or Public information, the resulting collection of information must be classified, at a minimum, as Confidential.

When **Internal Use Only** information is combined with Public information, the resulting collection of information must be classified, at a minimum, as Internal Use Only.

When information has not been explicitly classified as Restricted, Confidential, or Internal Use Only, the information by default shall not be considered as **Public**.

B. Integrity

The Integrity Protected classification indicates that the information, in electronic form, should be protected by Company-approved encryption or data inspection techniques that ensure the information has not been intentionally or inadvertently altered. Refer to the Integrity Protection Standard for specific instructions and information on proper controls to protect the integrity of Company information assets.

The Integrity Protected classification shall be applied with discretion to an information asset that if accidentally or intentionally altered without authorization would significantly damage the Company's competitive advantage and reputation or could lead to legal liabilities.

Possible examples of Integrity Protected information include:

Audit Logging, PII Data, SBU Data, CUI Data

C. Availability

All Company information shall be classified in one of three availability categories:

- High
- Medium
- Low

A description of each category is provided in the following table:

Availability Classification	Description	Potential Loss or Impact

High	High to continuous availability required. Examples may include: Back up systems, O365 Services, Active Directory, Critical IT Infrastructure Systems, CRM	Serious to severe impact. Examples may include: Examples may include: Significant Business Impact to the company and loss of essential services
Medium	Standard availability required. Examples may include: Support PAL, Security/Auditing logs, File Servers/Ports and Sharing, On-Boarding Systems	Limited to serious impact. Examples may include: Moderate financial loss, loss to business availability, customer service reduction
Low	Limited availability required. Examples may include: Marketing Sites	No critical impact. Examples may include: Minor losses or decline in customer service capability

D. Reclassification

Restricted information shall be reviewed for reclassification by the Asset Owner on a specific review date not to exceed five (5) years unless otherwise required by law or Company policy.

Confidential and Internal Use Only information shall be reviewed annually for reclassification. In accordance with Company procedures, this review may be conducted sooner in response to specific requests for reclassification.

E. Declassification

Restricted information shall be automatically declassified after five (5) years unless otherwise required by law or Company policy.

Declassification shall be performed in accordance with Company procedures.

3. Responsibilities

The Program Manager approves the Information Classification Standard. The Program Manager is also responsible for ensuring the development, implementation, and maintenance of the Information Classification Standard.

Company management, including senior management and department managers, is accountable for ensuring that the Information Classification Standard is properly communicated and understood within its respective organizational units. Company management also is responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the Information Classification Standard.

Asset Owners (Owners) are the 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. The Owner is responsible for defining processes and procedures that are consistent with the Information Classification Standard; coordinating with the Information Security Department to ensure that Company protection standards are properly established and maintained; and ensuring that accurate and updated information on network devices and servers in the production environment is retained.

Asset Custodians (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; coordinating with the Information Security Department to ensure that Company protection standards are properly established and maintained; configuring network devices, servers, and desktop systems in the Company production environment in accordance with established Company protection standards; retaining and updating accurate information on network devices and servers in the production environment; and cooperating with the Information Security Department and/or the Audit Department in efforts to check production servers for compliance to established Company protection standards.

Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for familiarizing and complying with the Information Classification Standard and associated guidelines; following Company-approved processes and procedures to request authorization to install hardware or software on their desktop or mobile system; ensuring desktop and mobile systems are available for automated updates; and maintaining the

confidentiality, integrity and availability of information accessed, consistent with the Owner's approved safeguards while under the User's control.

4. Enforcement and Exception Handling

Failure to comply with the Information Classification Standard and associated 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 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 Information 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