Information Systems and Technology Security

Information Handling 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

Information Handling Standard

The **22nd Century Technologies** (the "Company") **Asset Protection Standard** defines objectives for establishing specific standards for protecting the confidentiality, integrity, and availability of Company information assets.

This Information Handling Standard builds on the objectives established in the **Asset Protection Standard**, and provides specific instructions and requirements for handling information assets. These instructions address handling requirements for printed, electronically stored, and electronically transmitted information.

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.

- **Confidentiality classifications** are defined in the Information Classification Standard.
- **Information assets** are defined in the Asset Identification and Classification Policy.
- **Exchangeable media** refers to diskettes, tapes, removable hard drives, compact disks, etc.

2. Requirements

a. Printed Information

i. All printed information shall be handled based on its confidentiality classification. A description of handling requirements for each confidentiality classification category is provided in the following table:

	Restricted	Confidential	Internal use only	Public
Labeling				
Intra – company or office mail				
Duplication				
Mailing of documents				
Disposal				
Storage				

b. Electronically Stored Information

i. All electronically stored information shall be handled based on its confidentiality classification. A description of handling requirements for each confidentiality classification category is provided in the following table:

	Restricted	Confidential	Internal use only	Public
Labeling (application or screen)				
Labeling (electronic media)				
Stored on fixed media with access controls				
Stored on fixed media without access controls				
Disposal of electronic media				
Disposal of information				

c. Electronically Transmitted Information

i. All electronically transmitted information shall be handled based on its confidentiality classification. A description of handling requirements for each confidentiality classification category is provided in the following table:

	Restricted	Confidential	Internal use only	Public
Local area network				
Wide-area network				
Non-secure – public networks				
Electronic mail				
Fax				
Voicemail				

3. Responsibilities

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

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

Record Retention 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 Legal Hold Management 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; data storage devices issued by the company; and record handling systems in the production environment is retained. The Owner is responsible for identifying the various permeations that employees store and save information (i.e., some employees may save documents to a hard drive while others to a network file share).

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 and coordinating with administrators to ensure proper handling of information during processing and storage.

Record 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 record protection standards are properly established and maintained in accordance with established Company record hold standards.

Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for familiarizing and complying with the Information Handling Standard and associated guidelines, and handling information in manner that is consistent with the Information Handling Standard.

4. Enforcement and Exception Handling

Failure to comply with the Legal Hold Management Standard, Information Handling 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.

The following Case Request Form Sample illustrates the necessary key elements that should be preserved or considered if available during a litigation hold request event.

Case Request Form

This form should be completed and sent to Information Security when an asset must be forensically analyzed. **If possible, do not handle the asset without the assistance of an Information Security representative.** The Information Security department will assign the 22nd Century Technologies Case Number, Analyst Contact and Legal Contact. All other information should be completed by the requestor.

22nd Century Technologies Case number	
Date submitted:	
Time submitted:	
Legal consultation completion date:	

Case Subject and Requestor Information

Sensitivity classification:	[Restricted, Confidential, or Internal Use Only]
Person of interest:	
Employee number:	
Machine name:	
Analyst contact:	
Legal contact:	
Requester's name:	
Requesters employee number:	
Requesters title:	

Please check the spaces applicable to this legal hold request below. If specific information concerning the case is available, please supply this information in the **Keyword Search Parameters** spaces provided. Unless a full image is required, only selected data will be held.

Asset requested	Full data image	Specific data	Keyword Search parameters
Hard drive			
Network storage			
Removable storage devices			
Email			
Tablet			
Printer jobs			
Audit logs			
Mobile phone			
Mobile phone logs			
Voicemail logs			
Other			

Requester case details:

Information Security Analyst Findings:

Information hold location:	
Hold date:	
Case completion date:	
Accepted date:	
Accepted by:	

The Case Request Form may be obtained by contacting Information Security. Upon receipt of notice of significant defensive litigation and or material threat of litigation, the Chair of the Record Hold/Discovery Subcommittee shall direct the appropriate Company employee or employees to proceed with suspension of routine destruction of all relevant documents, to include, but not be limited to, email, communications, or other electronically stored data documents created by Company employees.

The General Counsel and or his designee shall notify employees of the Company identified as likely to have relevant information to the significant defensive litigation and or material threat of litigation of the need for the litigation or other legal hold and of their obligations to suspend routine record and other electronic document or physical document destruction.

Requests for exceptions to the Information Handling Standard should be submitted to the Company 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 Company CEO or its designee.

5. Review and Revision

The Information Handling 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