Information Systems and Technology Security

New Hire Security Awareness 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

New Hire Security Awareness Standard

The **22nd Century Technologies (the "Company) Security Awareness Policy** defines objectives for establishing a formal Security Awareness Policy, and specific standards for the education and communication of the Information Security Program Charter and associated policies and standards.

This New Hire Security Awareness Standard builds on the objectives established in the Security Awareness Policy, and provides specific instructions and requirements for providing security awareness education and training for newly hired Company employees.

1. Scope

All newly hired Company employees who have been granted access to Company information or systems are covered by this standard and must comply with associated guidelines and procedures.

- **Asset Owners** refers to the managers of organizational units that have primary responsibility for information assets associated with their functional authority.
- **Asset Custodians** refers to the managers, administrators and those designated by the Asset Owner to manage process or store information assets.
- **Electronic Communication Systems** refers to all Company information systems and equipment including Electronic Mail Resources, Internet Resources, and Telecommunications Resources.
- **Electronic Mail Resources** are defined in the Electronic Mail Acceptable Use Standard.
- **Information Assets** are defined in the Asset Identification and Classification Policy.
- **Internet Resources** are defined in the Internet Acceptable Use Policy.
- **Telecommunications Resources** are defined in the Telecommunication Acceptable Use Standard.

2. Requirements

a. General

i. Newly hired Company employees will receive the appropriate security awareness training as part of their formal new employee orientation.

ii. Newly hired Company employees should be oriented or trained in the following security areas:

- Company commitment to security
- Company Information Security Policy Framework
- Company information assets
- Confidentiality classification categories
- Information labeling
- User account and password requirements
- Remote access and mobile computing
- Physical access controls and requirements
- Virus prevention and detection
- Information Handling
- Proper use of software and Electronic Communications Systems
- Misuse Reporting
- Incident Reporting
- Help Desk and Information Security contacts

iii. Newly hired managers should receive the appropriate security awareness training in accordance with the Management Security Awareness Standard.

b. Policies

i. Information security awareness training for newly hired Company employees should cover the Information Security Program Charter and the following policies:

- **Asset Identification and Classification Policy**
- **Asset Protection Policy**
- **Acceptable Use Policy**
- **Security Awareness Policy**

ii. Information security awareness training for newly hired Company employees that are assigned Asset Owner or Asset Custodian responsibilities should also cover the following Company policies:

- **Asset Management Policy**
- **Vulnerability Assessment and Management Policy**
- **Threat Assessment and Monitoring Policy**

c. Standards

i. Information security awareness training for newly hired Company employees should cover the following standards:

- **Information Classification Standard**
- **Information Labeling Standard**
- **Access Control Standard**
- **Physical Access Standard**

- **Anti-Virus Standard**
- **Information Handling Standard**
- **Internet Acceptable Use Policy**
- **Electronic Mail Acceptable Use Standard**
- **Telecommunication Acceptable Use Standard**
- **Software Acceptable Use Standard**
- **Misuse Reporting Standard**
- **Ongoing Security Awareness Standard**
- **Security Awareness Accessibility Standard**

ii. Newly hired Company employees that have been granted remote access to Company information or systems to meet an approved business need or perform prescribed job responsibilities should receive information security awareness training that also covers the Remote Access Standard.

iii. Information security awareness training for newly hired Company employees that are assigned Asset Owner or Asset Custodian responsibilities should also cover the following Company standards:

- Integrity Protection Standard
- Encryption Standard
- Availability Protection Standard
- Life Cycle Management Standard
- Configuration Management Standard
- System Development Life Cycle Standard
- Change Control Standard

- Vulnerability Assessment Standard
- Vulnerability Management Standard
- Threat Assessment Standard
- Threat Monitoring Standard

3. Responsibilities

The Program Manager approves the New Hire Security Awareness Standard. The Program Manager also is responsible for ensuring the development, implementation, and maintenance of the New Hire Security Awareness Standard.

Company management is responsible for ensuring employees within their area of responsibility cooperate with Company security awareness and training efforts; ensuring that newly hired employees within their area of responsibility receive the proper Information Security awareness and training in accordance with the **Security Awareness Policy** and associated standards and guidelines; and ensuring the effective communication of relevant security issues with the Information Security Department.

4. Enforcement and Exception Handling

Failure to comply with the New Hire Security Awareness 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 New Hire Security Awareness Standard should be submitted to the 22nd Century Technologies 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 22nd Century Technologies CEO or its designee.

5. Review and Revision

The New Hire Security Awareness 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