

Information Systems and Technology Security

Third Party 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

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.

Third Party Security Awareness Standard

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

This Third-Party Security Awareness Standard builds on the objectives established in the **Security Awareness Standard**, and provides specific instructions and requirements for providing security awareness education and training for third party personnel.

1. Scope

Third party personnel 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 Standard.
- **Internet Resources** are defined in the Internet Acceptable Use Policy.
- **Telecommunications Resources** are defined in the Telecommunication Acceptable Use Standard.
- **Third party personnel** include contractors, partners, consultants, and other personnel that are not Company employees.

2. Requirements

a. General

i. Third party personnel should receive information security awareness training that covers the following security areas prior to being granted access to Company facilities, Company Electronic Communications System, and or Company information assets:

- Non-disclosure requirements
- Access limitations due to contractual agreement
- Company commitment to security
- Company information assets
- Confidentiality classification categories
- Information labeling
- User account and password requirements
- Physical access controls and requirements
- Virus prevention and detection
- Information Handling
- Proper use of software and Electronic Communications Systems
- Misuse Reporting
- Help Desk and Information Security contacts

b. Category Governance Standards

i. Third party personnel should receive information security awareness training that covers the Information Security Program

Charter, Information Systems and Technology Security Policy, and the following Company governance control standards:

- **Asset Identification and Classification Standard**
 - **Asset Protection Standard**
 - **Acceptable Use Standard**
 - **Security Awareness Standard**
- ii. Third party personnel that are assigned Asset Owner or Asset Custodian responsibilities should receive information security awareness training that also covers the following Company standards:

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

c. Standards

- i. Third party personnel should receive information security awareness training that covers the following Company standards:
- **Information Classification Standard**
 - **Information Labeling Standard**
 - **Access Control Standard**
 - **Physical Access Standard**
 - **Anti-Virus Standard**
 - **Encryption Standard**
 - **Information Handling Standard**

- **Internet Acceptable Use Policy**
 - **Electronic Mail Acceptable Use Standard**
 - **Telecommunication Acceptable Use Standard**
 - **Software Acceptable Use Standard**
 - **Misuse Reporting Standard**
 - **Security Awareness Accessibility Standard**
- ii. Third party personnel 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. Third party personnel that are assigned Asset Owner or Asset Custodian responsibilities should receive information security awareness training that also covers the following Company standards:
- **Integrity Protection Standard**
 - **Encryption Standard**
 - **Availability Protection Standard**
 - **Configuration Management Standard**
 - **System Development Life Cycle Standard**
 - **Change Control Certification Standard**
 - **Vulnerability Assessment Standard**
 - **Vulnerability Management Standard**
 - **Threat Assessment Standard**
 - **Threat Monitoring Standard**

3. Responsibilities

The Program Manager approves the Third-Party Security Awareness Standard. The Program Manager also is responsible for ensuring the development, implementation, and maintenance of the Third-Party 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 third party personnel within their area of responsibility receive the proper Information Security awareness and training in accordance with the **Security Awareness Standard** 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 Third-Party Security Awareness Standard and associated guidelines and procedures can result in disciplinary actions up to and including termination of contracts for contractors, partners, consultants, and other personnel. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Third-Party 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 Third-Party 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