Information Systems and Technology Security

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

Security Awareness Standard

As stated in 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 ensure that the **Information Security Program Charter** and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to facilitate awareness.

This Security Awareness Standard defines Company 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, standards, guidelines, and procedures.

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 policy 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.

2. Objectives

The Company **Information Security Program Charter** and relevant policies, standards and guidelines must be properly communicated to Company corporate and business unit management. Specific instructions and

requirements for providing security awareness education and training for Company management are provided in the **Management Security Awareness Standard**.

The Company **Information Security Program Charter** and relevant policies, standards, and guidelines must be properly communicated to and understood by all newly hired Company employees. Newly hired Company employees must be provided with the appropriate security awareness education and training. Specific instructions and requirements for providing security awareness education and training for new Company employees are provided in the **New Hire Security Awareness Standard**.

The Company **Information Security Program Charter** and relevant policies, standards, and guidelines must be properly communicated to and understood by all contractors, partners and consultants. Specific instructions and requirements for providing security awareness education and training for contractors, partners, and consultants are provided in the **Third-Party Security Awareness Standard**.

All Company employees will be provided with recurring and ongoing education and training to ensure continue awareness, and address emerging risks or topics of interest. Specific instructions and requirements for providing security awareness education and training for Company employees are provided in the **Ongoing Security Awareness Standard**.

All Company employees will be provided appropriate access to the **Information Security Program Charter** and relevant policies, standards, and guidelines. Specific instructions are provided in the Security Awareness Accessibility Standard.

3. Responsibilities

The CEO is the approval authority for the Security Awareness Standard.

The Program Manager is responsible for the development, implementation, and maintenance of the Security Awareness Standard and the associated standards and guidelines.

Company management is responsible for ensuring that the Security Awareness Standard and associated standards and guidelines are properly communicated and understood within their respective organizational units.

All individuals, groups or organizations identified in the scope of this standard are responsible for familiarizing themselves with and complying with the Security Awareness Standard and associated standards, guidelines, and procedures.

4. Policy Enforcement and Exception Handling

Failure to comply with the Security Awareness Standard and associated policies, 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 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 Security Awareness Policy will be reviewed and revised in accordance with the **Information Security Program Charter.**

Recommended: _____

Signature

Pakkirisankar Jagannath

Program Manager

Approved: _____

Signature

Anil Sharma

CEO