Information Systems and Technology Security

Incident Response Standard

Original author's name:	Pakkirisankar 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

Incident Response Standard

The **22nd Century Technologies** (the "Company) **Threat Assessment and Monitoring Standard** define objectives for establishing specific standards for assessing and monitoring threats to information assets.

This Incident Response Standard builds on the objectives established in the **Threat Assessment and Monitoring Standard**, and provides specific requirements for developing and exercising formal plans, and associated metrics, for responding to security incidents and intrusions. The Company will satisfy these requirements through a formal Security Incident Response Team (SIRT).

1. Scope

The Company SIRT will establish and maintain capabilities to respond effectively to electronic intrusions into the Company network infrastructure. SIRT analysis and planning activities will support proactive development of authorized, coordinated responses to incidents. The SIRT also will contribute to incident recovery activities after network intrusions are contained.

All SIRT members, as well as their management, are covered by the Incident Response Standard and must comply with its associated procedures and guidelines.

- **Information assets** are defined in the Asset Identification and Classification Standard.
- **Incident** refers to an anomalous event that may indicate a security intrusion.
- **Intrusion** refers to malicious activity on or directed toward a system, application, network, or network device.
- **Threats** are the intentional or accidental actions, activities or events that can adversely impact Company information assets, as well as the sources, such as the individuals, groups, or organizations, of these events and activities.

2. Requirements

a. General Requirements

i. **The Company shall develop a SIRT Concept of Operations (CONOP) that:**

- Summarizes the overall mission of the SIRT
- Defines the SIRT constituents and capabilities
- Defines the SIRT organizational structure
- Defines specific roles and responsibilities of SIRT members
- Summarizes the operational capabilities of the team

ii. The SIRT shall develop plans for responding to expected or typical types of intrusion events, as well as develop contingency plans for responding to new or unanticipated types of intrusions.

iii. The planned responses shall be dependent on the nature of the intrusion event and the criticality of the potentially impacted Company information assets.

iv. The SIRT shall maintain awareness of company information asset criticality definitions and shall develop incident response procedures that reflect these definitions.

v. The SIRT shall work with other departments as necessary to coordinate, in advance, responses that may directly impact those departments.

vi. SIRT planning activities shall address the full response spectrum. One end of the spectrum includes information logging as well as personnel notification and alerting. The other end of the spectrum includes higher profile responses (e.g., blocking access to the external web site, denying access from specific external networks, etc.).

vii. **The SIRT shall maintain metrics that address at least the following:**

- Incidents detected per reporting period, by severity category
- Average time from incident detection to response initiation
- Average time from response initiation to incident containment
- SIRT performance during exercises

b. Response Requirements

i. A SIRT Incident Response Procedure shall be developed to describe how to:

- Confirm assigned priority for valid incidents.
- Conduct or execute pre-coordinated response plans based on incident category.
- Determine if incidents have been contained.
- Perform basic forensic process to support security investigations.
- Ensure consistent and timely reporting of SIRT response activities.
- Document "lessons learned" to improve SIRT operations.
- Initiate SIRT recovery efforts, if necessary.

ii. The SIRT shall verify the existence of network and system intrusions, and take actions to contain the threat, in accordance with the SIRT Incident Response Procedure.

iii. The type of threat activity, together with the criticality of potentially impacted assets, shall provide the direct basis for conducting the incident response.

iv. SIRT members shall perform their designated, pre-coordinated tasks, in accordance with the SIRT Incident Response Procedure.

v. SIRT members shall meet periodically during the incident to check the status and effectiveness of the response.

vi. The SIRT shall coordinate with or notify impacted departments and external organizations as it conducts the incident response activities.

vii. The SIRT shall provide Company management with periodic status reports on the response activities.

viii. The SIRT shall transition to incident recovery activities when the incident or intrusion is contained and meets pre-defined SIRT recovery criteria.

ix. SIRT incident response capabilities shall be exercised, for evaluation purposes, at least annually. However, the SIRT members (with the possible exception of a senior SIRT manager) shall not be notified in advance of the exercises.

c. Recovery Requirements

i. A SIRT Incident Recovery Procedure shall be developed to describe how the SIRT will work within established business resumption and recovery capabilities.

ii. **The SIRT Incident Recovery Procedure shall describe how to:**

- Document SIRT damage assessment findings.
- Coordinate with Company departments or teams responsible for recovering impacted systems.
- Ensure consistent and timely reporting of recovery activities performed by the SIRT.
- Document "lessons learned" to improve SIRT operations.

3. Responsibilities

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

SIRT Managers are the members that have primary responsibility for managing and leading SIRT routine operations and incident response efforts associated with their functional SIRT assignments. SIRT managers are responsible collectively for securing the budget for resources to support the SIRT; interfacing with Company execute management and business owners; working closely with the management of the departments that are functionally part of the SIRT; arranging periodic SIRT exercises including incident simulation and intrusion drills for third-party verification of the SIRT operational and response capabilities; leading efforts to develop the SIRT organizational structure, procedures, and operational budget; conducting post-mortem evaluations to capture lessons learned; ensuring the ongoing execution and performance of SIRT procedures; arranging periodic training for SIRT members, and manage SIRT incident escalations; and ensuring that SIRT documentation is developed, approved, and distributed in a timely manner.

Core SIRT members are those designated representatives from key Company departments that have primary responsibility for performing SIRT routine operations and incident response efforts. Core SIRT members are responsible collectively for representing their respective departments in SIRT operations; communicating SIRT information within their departments; leading departmental support for SIRT activities; coordinating 7X24 departmental support to the SIRT; interfacing with local, state, and federal law enforcement agencies to facilitate legal responses to incidents; assisting with development of baseline IPS configurations; supporting reviews of available Information Security sources to maintain currency with information that can assist SIRT operations; and advising the SIRT, in concert with existing troubleshooting and status procedures, on strategies for processing non-routine notifications and responding to security incidents.

Supporting SIRT members are those designated representatives from key Company departments that supplement the core SIRT members by providing specific expertise or assistance. Supporting SIRT members are responsible collectively for representing their respective departments in SIRT operations; communicating SIRT information within their departments; leading departmental support for SIRT activities; providing legal advice to the SIRT and executive management; interface with management, employees, and contractors to facilitate personnel-related responses to incidents; assisting with internal communication on incident response and incident status information; leading

external communication to the media and public regarding responses to incidents; and supporting reviews of available Information Security sources to maintain currency with information that can assist SIRT operations.

Managers of SIRT members are responsible for working closely with SIRT management to ensure that their departmental representatives are performing their functionally assigned SIRT responsibilities, as well as the duties and tasks specified in approved SIRT procedures.

4. Enforcement and Exception Handling

Failure to comply with the Incident Response 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 Incident Response 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 Incident Response 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