SynPower Co., Ltd.

Information Security Incident Response and Reporting Procedures

Approved at the Board of Directors on held on September 19, 2024

I. Purpose

The Procedures are intended to provide clear guidelines for the Company in handling information security incidents. In the event of an incident, the established reporting procedures should be followed promptly, and necessary response measures should be taken to minimize potential impacts. Additionally, through incident handling and review, a learning mechanism can be established to reduce the likelihood and impact of similar incidents in the future.

II. Scope

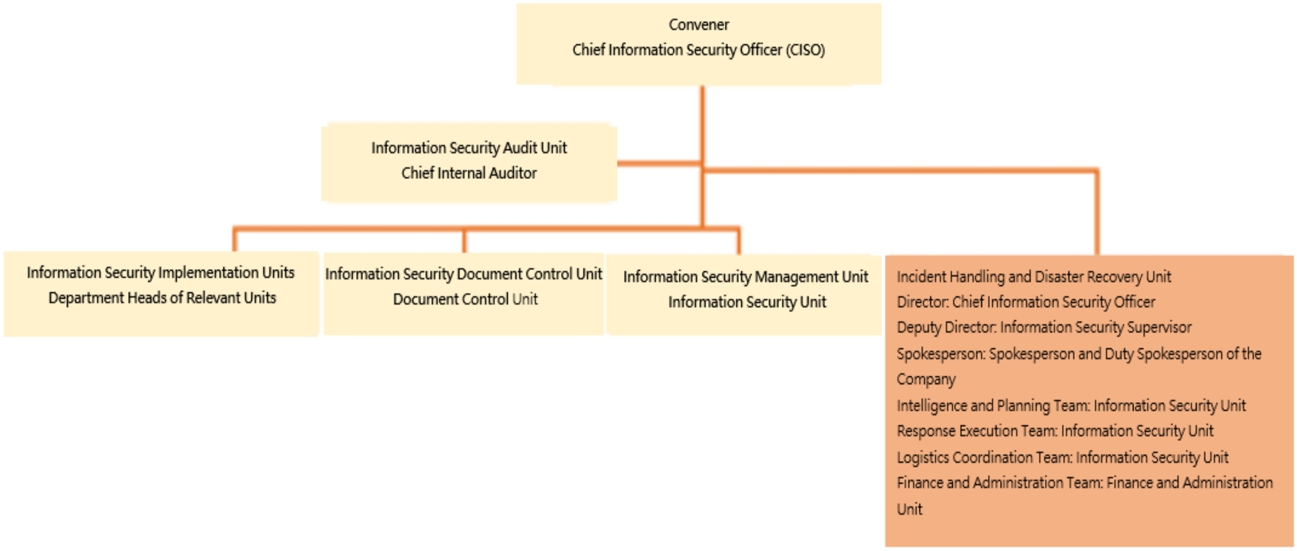
The Procedures apply to all employees, contractors, partners, and other third parties who access the Company's information assets, covering all information systems, networks, data, and related assets of the Company.

III. Definitions

1. Information Security Incident: Refers to any event that compromises the confidentiality, integrity, or availability of information or information and communication systems in the operating environment.
2. Discovering Personnel: Includes all Company members, whether full-time employees or non-regular personnel (such as temporary staff or assigned personnel), who are responsible for identifying and promptly reporting any suspected information security incidents.

IV. Information Security Organization

Information Security Management Organization


Convener
Chief Information Security Officer (CISO)
Information Security Audit Unit
Chief Internal Auditor
Information Security Implementation Units
Department Heads of Relevant Units
Information Security Document Control Unit
Document Control Unit
Information Security Management Unit
Information Security Unit
Incident Handling and Disaster Recovery Unit
Director: Chief Information Security Officer
Deputy Director: Information Security Supervisor
Spokesperson: Spokesperson and Duty Spokesperson of the Company
Intelligence and Planning Team: Information Security Unit
Response Execution Team: Information Security Unit
Logistics Coordination Team: Information Security Unit
Finance and Administration Team: Finance and Administration Unit

V. Roles and Responsibilities of the Information Security Organization

Title	Responsibilities
Convener	Held by the Company's Chief Information Security Officer (CISO), responsible for coordinating departments in the formulation and implementation of information security policies and objectives, as well as overseeing related management tasks. The chairperson presides over meetings, promotes and communicates cybersecurity topics, and reports the implementation status to senior management or the Board of Directors.
Dedicated Information Security Officer	Appointed by the Chairperson, this person is responsible for overseeing internal information security management. The officer monitors and reports on the Company's cybersecurity status, responds to external security

Title	Responsibilities
	control requirements, and handles related incidents.
Information Security Audit Unit	Appointed by the Audit Office, this unit is responsible for auditing the Information Security Committee and conducting internal and external information security audits to ensure compliance with relevant standards.
Information Security Implementation Units	Led by department heads of relevant units, these units are responsible for supporting and executing the Company's internal information security tasks in accordance with the directives of the Information Security Committee, ensuring alignment with security goals and decisions.
Information Security Document Control Unit	Managed by the document control department, this unit oversees the storage and version control of information security-related documents and ensures that the latest versions are provided to relevant departments.
Information Security Management Unit	Managed by the department in charge of information security, responsible for the daily operation, documentation, response, and maintenance of information security, ensuring continuity of security management efforts.

VI. Specific Management and Protection Measures

Member Role	Responsibility Description
Incident Director	Concurrently the Chief Information Security Officer (CISO), responsible for overall supervision, guiding various units to coordinate response efforts, and directly communicating with the company spokesperson.

Deputy Director	Assistant to the Incident Director, responsible for assisting in handling various tasks of the reporting and response team.
Spokesperson	The company-designated spokesperson, responsible for externally releasing incident-related information and regularly updating the reporting plan.
Intelligence and Planning Team	Composed of dedicated information security personnel or external experts, responsible for collecting and sharing security incident intelligence, and formulating response strategies and plans.
Response Execution Team	Composed of dedicated information security personnel or external experts, responsible for executing rescue and damage control work, assisting in system recovery, and reviewing vulnerability remediation after completion.
Logistics Coordination Team	Composed of dedicated information security personnel or external experts, responsible for ensuring the preservation of relevant data, assisting in incident cause analysis, and proposing improvement suggestions.
Finance and Administration Team	Composed of finance and administration units, responsible for budgeting and administrative support related to the incident.

VII. Information Security Incident Response and Reporting Procedures

1. Incident Discovery:

   When an information security incident is discovered or suspected, the discovering personnel shall promptly report the incident to the relevant Information Security Management Unit based on the circumstances and inform their direct supervisor.

1.1 Information Security Management Unit: Upon receiving the "Information Security Incident Report Form," the unit shall record and classify the incident based on the information provided by the discovering personnel.

1.2 Incident Assessment: After receiving the report, the Information Security Management Unit shall assess the incident to determine whether it qualifies as an information security incident. If deemed not to be one, the results will be communicated to the discovering personnel. If confirmed as an information security incident, the relevant responsible units and supervisors shall be notified for further handling based on the severity of the impact.

2. Classification of Information Security Incidents

Category	Incident Description
Natural Disasters	e.g., fire, earthquake, flood, typhoon, etc.
Data Center Facility Failure	e.g., uninterruptible power supply (UPS), power failure, or air conditioning system failure.
System Malfunction	1. Hardware failures, such as server breakdowns or hardware damage. 2. System/software anomalies, such as database service issues or ERP system errors.
Network Abnormalities	Network outages, such as inability to connect to internal or external networks.
Hacking Incidents	Cyberattacks causing system damage or disruption, such as ransomware, cryptojacking malware, or DDoS attacks.
Improper Personnel Operations	1. Personnel failing to follow relevant operating procedures. 2. Vendors or maintenance personnel not conducting proper risk assessments. 3. Intentional sabotage, human error, sensitive data leakage, or violations of information security policies.

Category	Incident Description
Computer or Peripheral Failures	Failure of personal computers, hardware, software, operating systems, power supply, networks, or peripheral devices.
Equipment Theft	Theft of equipment.
Others	Incidents that do not fall under the above categories.

3. Incident Documentation

3.1 The Information Security Management Unit must record detailed information when an incident occurs, including the situation of discovery, potential scope of impact, loss assessment, support requests, and response measures. All information must be documented in the "Information Security Incident Report Form."

3.2 The recorded information shall be provided to the Response Execution Team to assess the incident level, scope of impact, and loss estimation.

4. Incident Severity Classification

Level/ Incident Impact	Assessment Details
Level 4	1. Disclosure of confidential-level data 2. Core business systems or data severely tampered with or damaged 3. Severe impact on multiple business operations or systems, affecting the Company's reputation, with no timely recovery possible
Level 3	1. Disclosure of internal-access-only data 2. Impact on core business operations or interruption of related systems 3. Important business operations or systems affected, but recoverable within expected time frame
Level 2	1. General level incidents, involving non-core business systems 2. Minor data tampering, operational impact, or reduced system efficiency

Level/ Incident Impact	Assessment Details
	3. No impact on critical business operations or systems
Level 1	1. Non-core business assets 2. Very low level of impact or loss, with no effect on business or system operations

5. Incident Reporting

5.1 When an incident is discovered, the discovering personnel must immediately notify the Information Security Management Unit by phone. The reporting unit or the Information Security Management Unit shall then complete the “Information Security Incident Report Form” and submit it to the Response Execution Team.

5.2 The team must continuously update the responsible supervisors on the incident’s progress. Once the incident has been handled and normal operations restored, the results shall be recorded in the incident report and escalated according to the incident level.

5.3 If the incident involves stakeholders (or regulatory authorities or intelligence sharing institutions), reporting must be made according to the mechanisms stipulated or required by those stakeholders:

5.3.1 Notify stakeholders and keep a record of the reporting trail.

5.3.2 Assess the incident level based on contracts with stakeholders.

5.3.3 Hold a bilateral cybersecurity meeting if required by the stakeholders or the situation.

6. Incident Response Handling

6.1 For Level 4–3 incidents, the Director (Convener) shall lead; for Level 2–1 incident, the Deputy Director shall take charge. The Director shall establish an emergency response team as needed to eliminate or contain the abnormal event.

6.2 Level 4–3 incidents must be contained or restored within 36 hours; Level 2–1 incident must be contained or restored within 72 hours.

6.3 The targets of notification, methods of notification, and handling deadlines shall follow the table provided

Level/ Incident Impact	Command & Coordination	Notification Method	Resolution Timeframe
Level 4 (Severe)	Director	Phone or any available means of communication	Within 36 hours of notification
Level 3 (Major)	Director		Within 36 hours of notification
Level 2 (Moderate)	Duty Director		Within 72 hours of notification
Level 1 (Minor)	Duty Director		Within 72 hours of notification

7. Response to Unresolved Incidents

If the incident cannot be resolved within the predetermined recovery time:

7.1 The Information Security Management Unit (IT Department) shall be immediately notified. Within one hour, the facts and potential impact shall be clarified, and the incident level reassessed.

7.2 The revised scope, loss evaluation, incident level, classification, resource needs, emergency actions taken, and involved stakeholders shall be added to the "Information Security Incident Report Form." Assessment should also be made as to whether vendor assistance is needed.

7.3 If necessary and with supervisor approval, backup systems or emergency measures may be initiated based on the incident type and corresponding response procedure.

7.4 If the incident is classified as a Level 4 Major Security Incident, the commander shall establish a Major Information Security Emergency Response Team. In accordance with Article 34 of the "Guidelines for Information Security Management of TWSE/TPEx Listed Companies," a major information disclosure shall be made and reported in accordance with relevant regulations.

VIII. Incident Tracking and Investigation

1. After an incident occurs, the relevant information should be reviewed and analyzed to clarify the cause and responsibility of the incident, while assessing the risk of recurrence. Vulnerabilities in the current information environment should be examined and patched to prevent similar incidents

from happening again.

2. Relevant clues related to information security incidents should be properly preserved for future tracking and analysis.
3. To effectively track and review the cause of the incident, vulnerabilities in the existing environment should be carefully examined, and detailed information should be recorded in the "Information Security Incident Reporting Form."

IX. Review and Improvement Meetings

1. In the event of an information security incident classified as major or above, after the incident is handled and brought under control, the Incident Director shall convene relevant units or delegate the Deputy Director to chair a review meeting to deeply analyze the cause of the incident and prevent similar incidents from recurring.
2. Based on the review meeting results, the system owner shall implement corrective measures and perform necessary fixes to reduce the risk of recurrence.
3. Information security incidents should be incorporated into the "Information Security Incident Control Log" for case management and be regularly submitted for supervisory review along with the "Information Security Incident Reporting Form" and incident trace data.

X. Attachments

1. Information Security Incident Reporting Form — GP-MP-04701A
2. Information Security Incident Control Log — GP-MP-04702A