

## WNC Information Security Policy Statement

### 1 PURPOSE

- 1.1 WNC Corporation (hereinafter referred to as “the company”) provides comprehensive protection and precautions for information stored or transmitted by the company to eliminate information security risks such as destruction, theft, disclosure, tampering, misuse, and infringement, in order to uphold the company’s commitment to information security. The company establishes this Information Security Policy in accordance with international information security standards and specifications, including ISO/IEC 27001:2022 and TISAX, and implements the Plan-Do-Check-Act (PDCA) cycle to serve as guidelines for all personnel, ensuring the security of all information media.
- 1.2 The company’s information security objectives are “confidentiality”, “integrity”, “availability” and “legal compliance”. Relevant departments should establish and monitor their information security indicators to ensure that they align with the company’s Information Security Policy and regularly review whether they are achieved. All relevant departments shall establish and promote appropriate information security metrics and control measures in accordance with the company's Information Security Policy and overall objectives, regularly evaluate their execution effectiveness, and take necessary improvement measures based on evaluation results to continually maintain and enhance the effectiveness of the Information Security Management System (hereinafter referred to as the “ISMS”). Each unit shall review the suitability of its respective information security metrics at least once a year, and submit them for approval by the Information Security Committee and update relevant metric records in accordance with defined procedures.

### 2 APPLICABLE SCOPE

- 2.1 Applicable Site  
Applicable to our company and its affiliated enterprises and sites approved for inclusion in the scope of information security management.
- 2.2 Applicable Persons  
This security policy applies to all persons who access, use, or control IT facilities and services including, but not limited to, employees, contractors, temporary workers, visitors, vendors, and other workers at the company (including all personnel affiliated with third parties).
- 2.3 Applicable Standards and Requirements  
This policy conforms to applicable information security standards, specifications, and requirements, including but not limited to ISO/IEC 27001:2022 and TISAX management

requirements, and shall comply with applicable laws, regulations, customer contracts, and other requirements related to information security.

#### 2.4 Supplier

If a supplier is involved in accessing, processing, storing, or transmitting company information in the course of providing services, the supplier shall comply with the company's Information Security Policy, relevant ISMS regulations, and information security requirements specified in contracts and Statements of Work, and shall cooperate with the company to adopt necessary information security safeguards to maintain the confidentiality, integrity, and availability of information.

### 3 INFORMATION SECURITY POLICY STATEMENT

To ensure the effective operation of the company's ISMS and safeguard information assets across all operational locations within its scope of applicability, this policy statement is hereby promulgated as the overarching guiding principle for company-wide information security.

#### 3.1 Implementing information security to protect trade secrets

All IT and information operations shall ensure the confidentiality, integrity, and availability of information assets. Appropriate protection measures shall be selected for core trade secrets to mitigate the risks of unauthorized access, modification, destruction, and improper disclosure. The company shall implement appropriate protective measures for the safekeeping, storage, use, transmission, transfer, return, retirement, and disposal/destruction of information assets in accordance with their classification levels and relevant procedures. The viewing, use, access, and modification of information assets shall be restricted to authorized personnel and conducted strictly based on business needs and approved authorization. The company shall appropriately segregate duties based on business requirements and information security risks, and grant necessary permissions required to perform work duties based on personnel responsibilities and business needs. No personnel shall install, use, or download illegal or unauthorized software on company information assets.

#### 3.2 Strengthening product security to meet customer and market requirements

Security across all stages of the product lifecycle shall be supported. Product secure development, maintenance, and support processes shall be established and implemented, integrating product security requirements into stages including product requirements definition, design, implementation, testing, release, updating, and incident management. This aims to enhance product security quality and ensure process transparency, traceability, and quality

control. Detailed procedures shall be handled in accordance with the relevant product security procedures.

### 3.3 Regulatory compliance, Sustainability and business continuity

The company shall comply with applicable international standards, management requirements, customer contractual obligations, and information security laws and regulations, and establish IT Business Continuity and Disaster Recovery Plans based on the results of business impact analyses (BIA) and risk assessments. These plans are designed to assist the company respond to information security incidents, hacker attacks or intrusions, malware infections, unauthorized access, data leaks, network or IT system anomalies, and other security-related incidents, crises, and emergencies that may cause IT operation interruptions, business impacts, production downtime, financial losses, or other severe disruptions. When any of the aforementioned situations occur, reporting, emergency response, and recovery procedures shall be executed in accordance with relevant plans to minimize the impact on critical business operations and resume operations within the Maximum Tolerable Period of Disruption (MTPD).

In alignment with the sustainable development policy, the company duly takes into account factors such as resource utilization efficiency, energy conservation, environmental impact, and equipment lifecycle during the procurement, utilization, maintenance, and decommissioning of IT equipment and related services.

### 3.4 Information security education and training, total employee participation

The company shall conduct information security education, training, and guidance in accordance with the corporate training plan and procedure, and plan appropriate training topics based on personnel job functions, business requirements, and information security risks.

Training topics may include, but are not limited to, general information security awareness, social engineering prevention, and information security incident reporting and response; new hires shall be instructed to understand the Information Security Policy, the handling and response procedures for information security incidents, and relevant regulations. When necessary, the effectiveness of education, training, and awareness shall be evaluated.

### 3.5 Information security incident notification, response, and necessary disclosure

The company shall establish formal information security incident reporting procedures and communication channels. When company employees, external organizations having business relations with the company, or their personnel discover or suspect the occurrence of an information security incident, security vulnerability, or violation of the Information Security Policy and regulations, they shall promptly report it to the company. The responsible units shall

carry out necessary incident response measures based on the scope of impact and, when necessary, disclose relevant information to affected internal and external parties.

When a suspected information security incident occurs, an email shall be sent immediately to [security.issues@wnc.com.tw](mailto:security.issues@wnc.com.tw), or a report shall be made to the Information Security Incident Reporting Contact Window, describing the incident time of occurrence, symptoms/phenomena, and possible source to assist in determining whether it constitutes an information security incident and identifying the scope of affected IT operations.

Information security incidents shall be classified, responded to, handled, tracked, and closed in accordance with relevant procedures. If customers, partner vendors, regulatory authorities, or other external stakeholders are involved, necessary external reporting, progress notifications, and disclosures shall be handled in accordance with applicable laws and regulations, contracts, and company procedures. The head of the IR & Public Relations shall serve as the external spokesperson to centralize all external information releases.

Information security incidents shall be categorized into the following three levels based on the scope and degree of their impact. If an incident simultaneously meets the criteria of more than one level, the higher level shall apply:

- 3.5.1 Critical information security incident: An information security incident that causes major damage or impact to the company and reaches the threshold of regulatory reporting requirements.
- 3.5.2 Serious information security incident: An information security incident that affects the company's production or shipping, or directly impacts the company's reputation.
- 3.5.3 General information security incident: An information security incident that does not directly affect production, shipping, or company reputation.

Upon receiving a notification, the responsible unit shall immediately initiate response and handling in accordance with relevant procedures and complete the process within the specified time limits. For serious information security incidents, an Emergency Response Team shall convene relevant departments and complete the handling within 4 hours; for general information security incidents, handling shall be completed within 16 hours. If a general information security incident cannot be resolved within the specified time limit, the person shall immediately report it to his or her immediate supervisor, and escalation to a major information security incident shall be considered. Once an information security incident is confirmed, affected internal units shall be notified within 24 hours based on the incident classification and scope of impact; if customers, partner vendors, regulatory authorities, or other external

stakeholders are involved, the designated responsible unit shall execute necessary notifications, progress updates, and disclosures in accordance with applicable laws, regulations, contracts, and company procedures. Throughout the incident handling process, appropriate, timely, and necessary information shall be provided to affected internal and external stakeholders.

Following the completion of incident handling, the root causes, incident type, and scope of impact shall be reviewed based on relevant records, and corrective and mitigation measures shall be implemented to reduce the likelihood of recurrence.

### 3.6 Information security incident review and continual improvement

Following the completion of incident handling, the causes, incident type, and scope of impact shall be reviewed based on relevant records. Appropriate corrective measures shall be formulated and executed to reduce the likelihood of recurrence, and to continually enhance the effectiveness of the ISMS and incident handling. Lessons learned from incident post-mortems shall be fed back into IT Business Continuity and Disaster Recovery Plans in accordance with relevant procedures, and incorporated as needed into scenarios, emergency response procedures, and improvement items for subsequent Business Continuity Plan (BCP) or Disaster Recovery (DR) drills.

## 4 INFORMATION SECURITY MANAGEMENT OBJECTIVES

The company's Information Security Management Objectives refer to periodically evaluating the effectiveness of information security controls through objectives and quantifiable information security metrics, in order to maintain visibility over the operational status of the ISMS.

Each unit shall review the suitability of its respective information security indicators at least once a year and submit the review results to management review meetings for approval. Upon approval, an information security indicators summary sheet shall be updated in accordance with established procedures to serve as the information security indicators for the following year.

## 5 INFORMATION SECURITY RESPONSIBILITY

The company establishes an information security governance organization to clearly define the responsibilities of the Information Security Committee, the Information Security Department, all business units, users, and IT service providers, ensuring the effective operation and thorough implementation of the ISMS.

### 5.1 Information Security Committee

The Information Security Committee is responsible for the review and approval of information security management policies, strategies, and the ISMS, and shall perform the following duties:

- 5.1.1 Define the scope of the ISMS, and review information security policies, strategies, and relevant management standards.
- 5.1.2 Designate relevant personnel to conduct information security risk assessments, review risk assessment results and risk treatment strategies, and approve information asset classification, acceptable risk levels, applicable control measures, and required resources.
- 5.1.3 Approve information security indicators for each unit and review their achievement status.
- 5.1.4 Review internal audit results of the ISMS, monitor the progress of corrective and preventive actions, and track improvement status.
- 5.1.5 Review information security requirements from stakeholders, such as customer contracts, and verify that relevant requirements have been incorporated into the management of the ISMS.
- 5.1.6 Review information security incidents and their handling status, and approve relevant corrective or remedial measures when necessary.
- 5.1.7 Approve IT business continuity plans, business impact analysis results, and the required allocation of resources.
- 5.1.8 Convene or participate in ISMS Management Review Meetings to evaluate the suitability, adequacy, and effectiveness of information security policies, strategies, objectives, and the ISMS, and determine continual improvement initiatives as well as change requirements for the ISMS.

## 5.2 Information Security Execution Team

The Information Security Execution Team shall promote and execute ISMS-related management operations in accordance with the resolutions of the Information Security Committee, and consolidate implementation results and improvement status to submit to the Information Security Committee for review.

- 5.2.1 Conduct information security risk assessments and formulate risk treatment plans.
- 5.2.2 Assist the Information Security Committee in planning and establishing various control measures and operating procedures.
- 5.2.3 Promote and execute various ISMS control measures and operating procedures.
- 5.2.4 Consolidate and analyze various information security indicators of the ISMS.
- 5.2.5 Execute improvement items and corrective and preventive actions arising from internal and external information security audits.
- 5.2.6 Plan and implement information security education and training.
- 5.2.7 Identify applicable information security laws, regulations, and statutory requirements.

5.2.8 Conduct internal self-audits of the ISMS and track the improvement and remediation status of nonconformities.

5.3 Emergency Response Team

5.3.1 When a serious security incident occurs, convene relevant members and manage the review, response, coordination, contact, escalation, and investigation of the incident.

5.3.2 Lead the execution of an Emergency Response Plan and coordinate the allocation and utilization of resources.

5.3.3 Fully understand information about the incident to make decisions and handle escalations, and notify affected internal and external units, including customers and partner vendors, based on the scope of the effects.

5.3.4 Assemble the responsible personnel of each information service to develop, maintain, update, and perform recovery procedures of each information service.

5.3.5 Communicate and coordinate with DMIS related units and external vendors to ensure that there is adequate support equipment and required resources, and obtain urgently needed additional resources.

5.3.6 Assess damage at the incident site, direct the work on-site, be responsible for post- incident coordination, and perform recovery work at the original operating site.

5.3.7 Assist each unit in reviewing, confirming, and improving relevant structures post- incident; review the company's information security structure and provide improvement suggestions.

5.4 Information Security Audit Team

5.4.1 Information Security Audit Team Leader

5.4.1.1 Convene the information security audit team meetings.

5.4.1.2 Coordinate and allocate the tasks of internal auditing for ISMS.

5.4.2 Information Security Audit Team Member

5.4.2.1 Establish an internal audit plan for ISMS.

5.4.2.2 Perform internal audits for ISMS.

5.4.2.3 Prepare internal audit reports for ISMS.

5.4.2.4 Track non-conforming items and their improvement status.

5.5 All Departments and Users

5.5.1 All departments and users shall comply with the company's Information Security Policy, relevant ISMS regulations, and the information security requirements specific to their respective business operations.

5.5.2 All departments and users shall cooperate with the implementation of the ISMS, including information security education and training, audits, and relevant corrective and improvement actions.

5.5.3 Upon discovering suspected information security incidents, security vulnerabilities, or violations of information security policies and regulations, reports shall be filed promptly in accordance with relevant procedures.

5.5.4 All departments and users shall cooperate with the handling and remediation of information security incidents.

## 5.6 Service Providers

5.6.1 Comply with the company's Information Security Policy, relevant ISMS regulations, and contractual requirements.

5.6.2 Cooperate with information security risk assessments for outsourced operations and comply with related security requirements.

5.6.3 Comply with contractual specifications during the service period; if the service provided is of a long-term nature, service level reports shall be submitted regularly to the Business Owner for review and record in accordance with the requirements of the contract and Statement of Work.

5.6.4 Provide prior notice and obtain company approval before making any changes to personnel or operational scope.

5.6.5 Upon suspension or termination of services, return all company information assets and revoke relevant access privileges.

## 6 ISMS (Information Security Management System)

### 6.1 General Requirements

The company establishes, documents, implements, and maintains the ISMS in accordance with the requirements of ISO/IEC 27001:2022, ensuring that information assets and information systems are appropriately protected, and continually improving the effectiveness of the ISMS.

### 6.2 Operating Model

The company adopts the PDCA cycle to operate the ISMS, continually maintaining its effective operation through Plan, Do, Check, and Act.

#### 6.2.1 Plan

In accordance with the company's overall strategies and objectives, the ISMS is established by forming the Information Security Committee, controlling potential threats and

vulnerabilities, planning risk assessments, and designing and implementing control mechanisms.

6.2.1.1 Establish and maintain information asset inventory for information assets within the ISMS scope to serve as the basis for information asset management and risk assessment.

6.2.1.2 Evaluate asset values based on the confidentiality, integrity, and availability of information assets.

6.2.1.3 Evaluate the vulnerabilities of and threats to information assets based on existing control conditions, taking into account their potential impact.

6.2.1.4 Conduct risk assessments by synthesizing information asset values, vulnerabilities, and threats, and quantify the level of existing or potential risks faced by information assets to serve as the basis for selecting control measures.

6.2.1.5 Risk items exceeding the acceptable risk level shall be included in risk improvement plans, and appropriate control measures shall be selected based on the risk assessment results; the acceptable risk level, control measures, and required resources shall be approved by the Information Security Committee.

6.2.2 Do

Establish or modify requisite control mechanisms based on the results of assessment and planning.

6.2.2.1 Maintain various information assets within the ISMS scope, and establish and update Information Asset Inventory.

6.2.2.2 Clearly delineate safekeeping responsibilities for information assets, and designate appropriate information asset owners, custodians, and users.

6.2.2.3 Implement information asset classification and relevant protection requirements based on the confidentiality, integrity, and availability of the information assets.

6.2.2.4 Execute risk treatment and risk improvement plans in accordance with the acceptable risk level approved by the Information Security Committee.

6.2.2.5 For high-risk items exceeding the acceptable risk level, designate risk owners and remediation leads, and execute risk improvement plans.

6.2.2.6 Implement applicable control measures in accordance with the ISO 27001 Statement of Applicability.

6.2.2.7 Perform information security management operations in accordance with relevant ISMS policies, management procedures, and operational standards.

6.2.2.8 Asset inventory administrators of each unit shall review their responsible information asset inventory semi-annually; unit managers shall review and verify whether the information asset classification and inventory contents are updated to the current status.

6.2.2.9 Documents, forms, and records generated from ISMS operations shall be managed for document control, retention periods, and review/access authorization in accordance with documents control procedure.

### 6.2.3 Check

Monitor the thorough implementation of various operations within the ISMS, and evaluate and audit their effectiveness.

6.2.3.1 Information security metrics shall be objective and measurable indicators covering confidentiality, integrity, and availability, with defined metric descriptions, target values, measurement frequencies, data sources, and responsible personnel.

6.2.3.2 Each unit shall collect data, perform statistical analysis and evaluation, calculate information security metric values in accordance with the measurement frequency of each metric, retain relevant records, and obtain approval from the unit manager.

6.2.3.3 The designated personnel responsible for consolidating information security metrics shall aggregate metrics and relevant records from all units, and report the metric achievement status and analysis/evaluation results during Information Security Committee meetings.

6.2.3.4 Each unit shall review the suitability of its information security metrics at least once a year; upon approval by the Information Security Committee, information security indicators shall be updated to serve as the metrics for subsequent years.

6.2.3.5 Asset inventory administrators of each unit shall review the completeness, accuracy, and current status of information asset inventory semi-annually; unit managers shall review and verify information asset classification and inventory update status.

6.2.3.6 Risk assessment personnel shall conduct risk assessments semi-annually, incorporating existing control conditions, stakeholder requirements, and internal and external issues into the evaluation.

6.2.3.7 Management shall conduct ISMS internal audits at planned intervals to verify that control objectives, control measures, and related procedures conform to applicable standards, laws and regulations, and information security requirements.

6.2.3.8 The handling status of information security incidents shall be recorded and tracked; following the completion of incident handling, the causes of occurrence, incident type, and scope of impact shall be reviewed based on relevant records, and the ISMS shall be re-evaluated for any deficiencies.

6.2.3.9 Perform the daily operations of the Security Operations Center (SOC) and continuously monitor and measure the operation of information security management and technical protection, including information security system management, monitoring, analysis of suspected abnormal behaviors, alert handling, and review of relevant records. Management-level and technical-level monitoring and measurement shall be carried out concurrently. Based on the monitoring and analysis results, abnormalities shall be tracked and risks shall be assessed. Where necessary, the company shall coordinate with relevant units to respond to, analyze, handle, mitigate, and improve information security incidents.

#### 6.2.4 Act

Based on the results and recommendations of monitoring and audits, execute corrective actions, improve and implement requisite control mechanisms, and continually maintain the operation of the ISMS.

##### 6.2.4.1 Continual Improvement

6.2.4.1.1 Continually improve the effectiveness of the ISMS through internal and external audit results, information security incident analysis, corrective actions, and management reviews.

6.2.4.1.2 Following the completion of incident handling, the causes of occurrence, incident type, and scope of impact shall be reviewed based on relevant records to re-evaluate the ISMS for any deficiencies and adopt necessary corrective measures.

6.2.4.1.3 If necessary, improvement proposals or new control measures shall be submitted and presented to the management review meetings for approval in accordance with relevant procedures.

##### 6.2.4.2 Corrective Actions

6.2.4.2.1 For nonconformities identified during the establishment and operation of the ISMS, root causes shall be identified.

6.2.4.2.2 Evaluate actions to be taken to ensure that nonconformities do not recur.

6.2.4.2.3 Determine and implement necessary corrective actions.

6.2.4.2.4 Record the results of executed corrective actions and review their effectiveness.

#### 6.2.4.3 Management Review

6.2.4.3.1 The Information Security Committee shall conduct a management review at least semi-annually to ensure the suitability, adequacy, and effectiveness of the ISMS.

6.2.4.3.2 The management review shall take into consideration the following: follow-up actions from previous management reviews; changes in the internal or external environment that could affect the ISMS; feedback on the information security performance; feedback and requirements from interested parties; risk assessment results and the status of risk-mitigation plans; and other suggestions for continual improvement.

6.2.4.3.3 The management review shall evaluate opportunities for continual improvement and need for changes to the ISMS, including changes to the Information Security Policy and Information Security Objectives.

6.2.4.3.4 The results of the management review shall be documented in detail and properly retained.

### 6.3 Control of ISMS Documents and Records

#### 6.3.1 Document Control

6.3.1.1 ISMS-related documents shall be established in accordance with document classification and numbering rules, and the drafting, approval and issuance, revision, retention, and distribution methods of documents shall be clearly specified.

6.3.1.2 When an ISMS document is created, revised, or cancelled, the designated responsible unit shall conduct a review and the document shall only take effect upon approval by the authorized manager.

6.3.1.3 When revising documents, the document version and revision details shall be identified; document versions shall be managed in accordance with document content procedure, and revision details shall be documented accurately and comprehensively.

6.3.1.4 The issuance and access of ISMS documents shall be controlled according to authorization hierarchies to ensure that applicable units obtain the current valid versions. When a paper document is revised, the previous version shall be recalled and replaced with the new version in accordance with the Document Control Procedure. Documents cancelled and retained for regulatory, technical, knowledge

preservation, or other requirements shall be clearly marked as “Cancelled” for identification. Cancelled document versions that are not required to be retained and storage media containing information assets shall be subject to appropriate data erasure, degaussing, destruction, shredding, or other disposal methods according to their confidentiality levels, media types. Among these methods, the destruction methods for paper or document-type media shall refer to ISO 21964 Level 4 and Level 3, respectively. The destruction of materials classified as industrial waste shall be handled in accordance with the industrial waste storage and clean-up control procedure.

6.3.1.5 External documents shall be identified, requested, retained, and controlled; original electronic files or hard copies shall be archived and retained by the DCC.

6.3.1.6 Documents shall be properly maintained and protected against the leakage of confidential information. The recall, destruction, and related records of obsolete documents shall be handled in accordance with document control procedure and Section 6.3.1.4 of this policy. Older versions of documents retained for regulatory, technical, knowledge preservation, or other requirements shall be stamped “Void” or clearly identified by other appropriate means to prevent misuse.

#### 6.3.2 Record Control

6.3.2.1 Forms and records generated during ISMS operations shall comply with relevant requirements for document numbering, revision control, retention, and access management.

6.3.2.2 The distribution, recall, borrowing, and destruction of documents shall be carried out in accordance with the document control procedures, and necessary document control records shall be retained. The retention, inspection, and access of relevant records shall be managed in accordance with document control requirements.

## 7 MANAGEMENT RESPONSIBILITY

### 7.1 Management Commitment

To ensure the effective operation of the ISMS, management shall:

7.1.1 Approve, communicate, and oversee the Information Security Policy, and ensure that information security responsibilities are appropriately assigned and coordinated.

7.1.2 Promote, coordinate, and supervise information security management matters through the information security governance organization.

7.1.3 Ensure that Information Security Objectives are aligned with the direction of the company's Information Security Policy, and regularly review their achievement status.

7.1.4 Approve the acceptable risk level in accordance with information assets and risk assessment management procedure, and approve control items and required resources based on risk assessment results.

7.1.5 Management shall supervise the execution of information security risk assessments and ISMS internal audits, and the Information Security Committee shall conduct ISMS management reviews.

7.1.6 The Information Security Committee shall conduct a management review at least semi-annually to evaluate the suitability, adequacy, and effectiveness of the ISMS.

## 7.2 Resource Management

Management shall provide the resources needed for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the ISMS, and ensure that information security personnel fulfill their responsibilities.

Information security education, training, and awareness shall be handled in accordance with the educational training procedure.

## 7.3 Effective Communication

The company shall determine internal and external communications relevant to the ISMS based on internal and external issues as well as the needs and expectations of interested parties/stakeholders, ensuring that the Information Security Policy, objectives, responsibilities, and relevant requirements are appropriately communicated and conveyed.

# 8 INTERNAL AUDIT

8.1 The company shall conduct an ISO 27001 ISMS internal audit at least once a year. In the event of serious information security incidents, major nonconformities, or other necessary circumstances, ad-hoc audits may be conducted in accordance with the internal audit procedure. The audit shall verify the conformity and effectiveness of the ISMS, its control objectives, control measures, and relevant procedures.

8.2 Internal audits shall be conducted in accordance with the audit plan, scope, criteria, and methods defined in the internal audit procedure.

8.3 For nonconformities identified during internal audits, their root causes shall be identified, necessary corrective actions shall be evaluated and determined, and the effectiveness of corrective actions shall be recorded and reviewed.

- 8.4 The results of internal audits and the status of improvements shall be submitted to the Information Security Committee for review, serving as the basis for ISMS continual improvement and management reviews.

## 9 ISMS MANAGEMENT REVIEW

### 9.1 Review Frequency and Convening

The Information Security Committee shall convene a Management Review Meeting semi-annually. When necessary, extraordinary meetings may be convened, or reviews may be conducted via written circulation/document review. The meetings shall be convened by the convener of the Information Security Committee.

### 9.2 Review Content

Management reviews shall be conducted in accordance with the ISMS and relevant procedures to review the information security policy, strategy, ISMS-related regulations, information security objectives, and their implementation status, and shall consider the following:

- 9.2.1 Follow-up actions from previous management reviews.
- 9.2.2 Changes in internal or external issues and the environment that could affect the ISMS.
- 9.2.3 Feedback on the implementation of the ISMS, including the achievement of Information Security Indicators, ISMS audit results, information security incidents, and improvement measures.
- 9.2.4 Feedback and requirements from interested parties.
- 9.2.5 Risk assessment results and the status of risk handling plans.
- 9.2.6 Other suggestions for continual improvement.

Management reviews shall also examine the information security policy, strategy, ISMS-related regulations, information security objectives, and their implementation status, and evaluate the continuing suitability, adequacy, and effectiveness of the ISMS. The Personnel-in-charge of consolidating Information Security Indicators shall explain the statistical analysis and evaluation results at meetings of the Information Security Committee. When an Information Security Indicator fails to achieve its target value, corrective actions shall be taken.

### 9.3 Review Outputs

The results of the management review shall include decisions related to continual improvement opportunities, needs for changes to the Information Security Policy, objectives, or the ISMS, adjustments to risk treatment or control measures, and resource needs.

### 9.4 Review Decisions and Records

Based on the review results, the management review shall determine continual information security improvements, ISMS change requirements, and the provision methods and scope of

resources. The meeting proceedings shall be documented, properly retained upon approval, and protected in accordance with the classification level of information assets.

## 10 ISMS IMPROVEMENT

### 10.1 Initiation of Improvement Measures

The company shall identify improvement needs based on information security incidents, risk assessment results, and the achievement status of information security metrics, and take corrective actions or risk improvement measures in accordance with relevant procedures.

### 10.2 Implementation of Improvement Measures

Upon completion of risk improvement measures, risks shall be re-evaluated in accordance with information assets and risk assessment management procedure. Risk identification and risk reduction measures shall continue to be executed based on the evaluation results until risks are reduced to an acceptable level.

Non-conformities identified during internal audits shall be handled in accordance with internal audit procedure for auditing, improvement follow-up, and verification. Non-conformities identified during internal or external audits shall be handled in accordance with corrective and preventive action procedures to complete cause analysis, corrective actions, and necessary preventive actions. The responsible personnel shall track the implementation status of improvement actions and verify their effectiveness. Any actions that have not been completed, or whose effectiveness has not yet been confirmed, shall continue to be tracked until the improvement is completed and verified.

### 10.3 Corrective of Improvement Measures

Corrective actions taken when information security metrics fail to achieve target values shall explain the root causes, execute corrective actions, and track handling status and improvement results in accordance with information security indicator management procedure; when necessary, fill out corrective action form.

### 10.4 Tracking of Improvement Measures

The results of implementing improvement measures shall be recorded and tracked, and the effectiveness of the improvement measures shall be verified in accordance with relevant procedures. When an Information Security Indicator fails to achieve its target value, information security indicator management procedure shall be followed to complete corrective action form, and the processing status and corrective actions of the responsible unit shall be tracked. Improvement measures for information security incidents shall be handled in accordance with information security incident management standard to confirm whether the

impact of the incident and the likelihood of recurrence have been reduced, and shall serve as a basis for management reviews conducted by the Information Security Committee and the continual improvement of the ISMS.

## 11 PENALTIES

- 11.1 Company personnel (including regular employees, contract employees, dispatched workers, and temporary employees) shall strictly comply with this policy and related information security regulations. Any violation of information security regulations or acts causing damage to company assets shall be disciplined in accordance with the company's general rules for employee rewards and punishments. In cases of severe violations involving illegal acts, the company shall pursue civil and criminal legal liabilities in accordance with the law.
- 11.2 If visitors, suppliers, or personnel from external partner organizations violate this policy or the information security requirements stipulated in relevant contracts, such matters shall be handled in accordance with applicable contract terms, Statements of Work (SOW), or legal regulations. Furthermore, the company reserves the right to terminate cooperation and pursue claims for damages.

## 12 REVIEW and ISSUANCE for IMPLEMENTATION

Upon review and approval by the authorized manager, this Information Security Policy Statement shall be promulgated, distributed, and controlled in accordance with document control procedure to ensure that personnel obtain applicable and valid document versions.

The company shall conduct education, training, and awareness campaigns regarding the Information Security Policy, information security incidents, and relevant regulations in accordance with education training procedure; new hires/personnel shall undergo training on relevant information security policies and regulations.