EIKEI Group (Cayman) Co., Ltd.

榮惠集團(開曼)股份有限公司

Information Security Operating Procedures

資通安全作業程序

December 2023

Information Security Operating Procedures

Contents

A. Basis and Purpose

This plan is formulated in accordance with Article 10 of the Information Security Management Act and Article 6 of the Enforcement Rules.

B. Applicability

This plan applies to the entire group and its subsidiaries.

C. Core Business and Significance

a. Core Business and Significance：

The core businesses and significance of the group are as follows：

Core Business	Core Information Systems	Significance Explanation	Impact on Business Failure	Core Business Recovery Time Objectives	Data Recovery Point Objectives	Maximum Tolerable Downtime
Group Enterprise Operational Processes	ERP System	Critical business operations for the group's maintenance	Impact on the group's operational activities	48 hours	2 hours	64 hours

Field Definitions：

1. Core Business Name: Please refer to the provisions of Article 7 of the Enforcement Rules of the Information Security Management Act for listing。
2. Importance Explanation: Explain the importance of the business to the corporate group, such as its impact on group finances and reputation, legal compliance implications, or other explanations of significance.
3. Identify the probability of potential operational disruption events and assess their impact. Establish the Recovery Time Objectives (RTO) and the Recovery Point Objectives (RPO) for core business operations.
4. Maximum Tolerable Downtime expressed in working hours (with one day equivalent to 8 hours).

b. Non-Core Business and Explanation：

The non-core business of this group and its explanation are as follows in the table below：

Non-Core Business	Business Failure Impact Explanation	Maximum Tolerable Downtime
Group Network Management and Maintenance	Impact on Group Service Connectivity Operations during Network Service Disruption	40 hours
Document Management System	Impact on Group Connectivity Access to Relevant Document Content during Service Outage	16 hours

Field Definitions：

1. Business Name: The non-core business of the corporate group should include at least the business names of supporting units, such as attendance services, mail services, client services, etc. (Please list based on the actual situation of the group)
2. Maximum Tolerable Downtime measured in working hours (with one day equivalent to 8 hours).

D. Information Security Policy and Objectives

a. Information Security Policy

To ensure the smooth operation of our group's business and prevent unauthorized access, use, control, disclosure, destruction, alteration, or other infringements of information or information systems, and to ensure their confidentiality, integrity, and availability, the following policy is established for all employees to adhere to collectively：

1. In response to changes in the Information Security threat landscape, all personnel in our group should participate in Information Security education and training to enhance Information Security awareness.
2. Relevant personnel should ensure familiarity with the Information Security incident reporting mechanism and effectively complete reporting procedures.
3. Conduct regular internal audits to ensure the proper implementation of relevant operations.

4. Ensure that the group's network services maintain a level of availability at 99.5%

b. Information Security Objectives

i. Quantitative Objectives

1. All personnel in the group complete 1 hour of Information Security education and training annually. ◦
2. Awareness of Information Security incidents, completing reporting, response, and closure operations within the specified time. The group should have less than 1 occurrence of being aware of an Information Security incident but not reporting it annually.
3. The number of unresolved improvement items from the previous internal audit should be less than or equal to 3.
4. The number of unplanned network service disruptions per year, with each occurrence exceeding 4 hours, should be less than or equal to 5.

c. Approval Process for Information Security Policy and Objectives

The Information Security policy is approved by the head of the Information Security Department. After confirmation by the relevant departments, it is then approved by the General Manager before being published.

d. Promotion of Information Security Policy and Objectives

1. The Information Security policy and objectives of the group should be promoted annually to all personnel within the group through education and training, internal meetings, posted announcements, and other notification methods. The effectiveness of implementation should also be reviewed.
2. The group should annually promote Information Security policies and objectives to stakeholders (such as IT service providers and units related to group connectivity operations) and review the effectiveness of implementation.

e. Regular Review Process for Information Security Policy and Objectives

The Information Security policy and objectives should be regularly reviewed for their appropriateness, and any adjustments require approval from the Chief Information Security Officer.

E. Organization for Promoting Information Security

a. Chief Information Security Officer (CISO)

In accordance with the provisions of Article 11 of this law, the Chief Information Security Officer is established to oversee Information Security matters within the group. Their responsibilities include：

1. Approval, coordination, and supervision of Information Security management policies and objectives.
2. Allocation and coordination of Information Security responsibilities.
3. Allocation of Information Security resources.
4. Supervision of Information Security protective measures.
5. Review and supervision of Information Security incidents.
6. Approval of Information Security-related regulations, procedures, and institutional documents.
7. Approval of the annual work plan for Information Security management.
8. Supervision and performance management of Information Security-related tasks
9. Approval of other Information Security matters.

b. Information Security Promotion Team

To promote the group's Information Security policies, implement Information Security incident reporting, and handle related response measures, the Chief Information Security Officer appoints personnel responsible for the Information Security promotion team. Their tasks include：

1. Coordination of responsibilities and tasks related to Information Security matters across departments.
2. Coordination and deliberation on the adoption of Information Security technologies, methods, and procedures.
3. Coordination and deliberation on overall Information Security measures.
4. Coordination and deliberation on Information Security plans.
5. Deliberation on Information Security policies and objectives.

6. Formulation of group Information Security regulations, procedures, and institutional documents, ensuring their compliance with legal and contractual requirements.
7. Development of the group's annual work plan based on Information Security objectives.
8. Dissemination of the group's Information Security policies and objectives.
9. Research, implementation, and evaluation of Information Security technologies.
10. Implementation of Information Security regulations, procedures, and institutional documents.
11. Inventory and risk assessment of information and information communication systems.
12. Implementation of security measures for data and information communication systems.
13. Execution of Information Security incident reporting and response mechanisms.
14. Conducting internal audits of Information Security.
15. Annual reporting on the implementation status of the Information Security maintenance plan.

The list of personnel and their responsibilities in the group's Information Security promotion team should be filled out in the " Information Security Promotion Team Member Planning Explanation and Assignment Sheet " document, and it should be updated as needed.

F. Allocation of Human and Funding resources

a. Allocation of Human Resources and Resources for Information Security

1. The group, according to the classification method specified in the Information Security guidelines, falls under the second level of Information Security. One dedicated manager for information communication and one dedicated personnel for Information Security are appointed. The roles of these personnel should be filled out in the " Information Security Promotion Team Member Planning Explanation and Assignment Sheet " document, and it should be updated as needed.

2. When the operational units of the group handle Information Security human resource tasks, they should strengthen the training of Information Security personnel and enhance the Information Security management capabilities of Information Security professionals within the group. If there is a lack of Information Security manpower or experience in relevant units of the group when handling Information Security tasks, consulting services may be sought from relevant scholars, experts, or professional groups.

3. Personnel responsible for the management, maintenance, design, and operation of critical information and communication systems within the group should have appropriate division of labor and decentralized responsibilities. Those with responsibilities for confidential maintenance should sign relevant confidentiality agreements upon entry, and a human resource backup system should be established.

4. Senior executives and business managers at all levels within the group should be responsible for supervising the Information Security operations of their subordinates and preventing illegal and improper conduct.

5. The configuration of professional human resources should be reviewed regularly on an annual basis.

b. Allocation of funds

1. The Information Security Promotion Team, when planning the allocation of relevant funds and resources, should consider the Information Security policies and objectives of the Group. They should also provide resources needed to establish, implement, maintain, and continually improve the Information Security Maintenance Plan.

2. When planning the construction of information and communication systems, the Group should concurrently plan the Information Security protection requirements of these systems. The Information Security budget should be reasonably allocated or evenly distributed within the overall budget.

3. If there is a need for Information Security resources, it should be submitted to the Information Security Team through internal endorsement or by completing the "Information Security Requirement application Form." The Information Security Promotion Team will allocate resources based on overall Information Security needs. After approval by the Chief Information Security Officer (CISO) and submission to the Group CEO, relevant implementations will proceed accordingly.

4. The allocation of Information Security funds and resources should be reviewed periodically on an annual basis.

G. Inventory of Information / Information Communication System

a. Inventory of Information / Information Communication System

1. The group conducts an annual inventory of information / information communication system assets. Responsible personnel are assigned based on management responsibilities, and assets are classified according to their attributes, including information assets, software assets, physical assets, and support service assets.
2. The items of information and information communication system assets are as follows：
   (1) Information Assets: Information stored in digital or other forms, such as Office electronic files, databases, etc.。
   (2) Software Assets: Application software, system software, development tools, packaged software, and computer operating systems, etc.。
   (3) Physical Assets: Computers and network equipment, portable devices, etc.。
   (4) Personnel Assets: System administrators, equipment managers, outsourced on-site vendors, etc.。
3. Each year, the Group should create an "Inventory of Information and Communication System Assets" based on the results of the information and communication system inventory. The fields should include serial number, information system name, business attributes, information system security level, responsible unit, and remarks.
4. Responsible Unit: The unit with management responsibilities for the asset.
5. Physical assets are managed in accordance with the Fixed Assets Regulations.
6. In case of any changes to the information or information and communication systems managed by each unit, the Information Security Promotion Team should be promptly notified to update the " Inventory of Information and Communication System Assets. "

H. Information Security Risk Assessment

a. Information Security Risk Assessment

1. The Group shall conduct a risk assessment for information and communication system assets annually and complete the "Risk Assessment Form."。

2. The risk assessment items and calculation formulas are as follows：

   (1) Asset risk calculation needs to consider asset value (C+I+A), likelihood, and impact.。

   (2) Asset value = [Confidentiality (C) + Integrity (I) + Availability (A)] of the asset.。

   (3) Asset risk = Asset value (C + I + A) × Likelihood × Impac

   (4) Risk Distribution：

Low Risk	Medium Risk	High Risk
3~37	38~73	74~108

   (5) When the asset risk is assessed as high, the "Risk Improvement Plan Form" should be filled out for risk improvement operations.

3. The asset value should consider confidentiality (C), integrity (I), and availability (A). Please refer to the "Asset Value Assessment Form" for evaluation criteria.

4. The calculation of asset risk requires assessing the likelihood and impact of each event. Please refer to the "Likelihood and Impact Assessment Form" for evaluation standards.

5. Threat and Vulnerability Assessment：

   (1) Assets subject to threat and vulnerability assessment are categorized into five types based on potential events (threats-vulnerabilities). Please refer to the "Threat Vulnerability Mapping Table," including the following categories：

      01 Information Asset Risk: Includes risks arising from the improper creation, maintenance, control, and transmission of data and documents.

      02 Software Asset Risk: Includes risks arising from improper system

design, maintenance, and operation.

03 Physical Asset Risk: Includes risks arising from the lack of physical security controls or inadequate environmental monitoring.

04 Risk of Support Service Assets: Includes risks arising from insufficient capacity or improper maintenance.

05 Risk of Personnel Assets: Includes risks arising from intentional or unintentional actions of personnel, inadequate security training, etc.

I. Information Security Protection and Control Measures

Based on the previous chapter's results of Information Security risk assessment and the assigned responsibilities according to its Information Security responsibility levels, the Group implements the following protection and control measures:

a. Access Control and Encryption Mechanism Management

i. Network Security Management

1. Users are not allowed to privately install computers and network communication equipment in the office.
2. Users should adhere to network security regulations. In case of any violation of network security, access rights may be restricted or revoked in accordance with Information Security regulations.

ii. Permission Management

1. The password setting policy should avoid using easily guessable or personal information. ◦
2. User account privileges should be opened according to the user's business needs, and shared accounts are not allowed.
3. When users no longer need to use information and communication systems, their accounts should be promptly deactivated or removed.

iii. Encryption Management

1. Encryption should be applied to confidential information during storage or transmission.
2. Encryption protection measures should avoid retaining decryption information. If there are signs of encryption compromise, it should be changed

immediately.

b. Operational and Communication Security Management

i. Measures to Prevent Malicious Software

1. The group's servers and personal computers should have antivirus software installed, and software and hardware maintenance should be performed regularly.
2. Any files obtained from storage media in any form should be checked for malicious programs or viruses.
3. Users are not allowed to install software from unknown sources, with legal concerns, or unrelated to business without permission.

ii. Email Security Management

1. Users should exercise caution when using email, avoiding opening emails from unknown sources.
2. In principle, confidential or sensitive information should not be transmitted via email. If there is a business need, encryption or other protective measures should be applied according to relevant regulations.
3. Users are not allowed to use the email services provided by the group for activities that infringe upon the rights of others or engage in illegal behavior.
4. The group should cooperate with the higher-level group to conduct email social engineering drills and review the execution.

iii. Ensuring Physical and Environmental Security Measures

1. Adopting a clean desk policy should be considered to reduce the risk of unauthorized access, loss, or damage to confidential information, documents, and removable media outside office hours.
2. Information or communication system-related equipment should be stored securely and must not be taken out of the office without authorization from the responsible personnel.

iv. Media Protection Measures

1. When using storage devices such as USB drives or disks to store data, confidential and sensitive information should be securely handled.
2. When transmitting information using physical storage media, attention should

be paid to the packaging of the physical storage media, and appropriate personnel should be selected for the transfer.

v. Security Management for Personal Computer Usage

1. When the personal computer is not in use, it should be logged out immediately or the screen lock function should be activated.
2. Installation and use of unauthorized software are prohibited.
3. Personal computers should undergo regular updates for the operating system, application patches for vulnerabilities, and antivirus definitions.
4. In case of discovering Information Security issues, one should actively report them through the group's notification procedure.
5. Important data should be regularly backed up.

c. Information and Communication Security Protection Equipment

i. Firewalls should undergo timely software and hardware updates and maintenance operations.

ii. Firewall configuration files should be backed up as needed.

J. Mechanisms for reporting, response, and drills of Information Security incidents.

To promptly manage information and communication security incidents and minimize damages, the group should establish mechanisms for reporting, responding to, and practicing drills, as outlined in the " Information security Incident Reporting and Incident Response Management Procedures" ◦

K. Assessment and response to information and communication security intelligence.

Upon receiving information and communication security intelligence, the group should assess its content, consider its impact on the group, acceptable risks, and available resources. The most appropriate response should be determined, and if necessary, adjustments to the control measures in the information and communication security maintenance plan may be made, with records kept accordingly.

a. Classification and assessment of information and communication security

incidents.

After receiving information and communication security incidents, the group should designate dedicated personnel to analyze the intelligence. The classification and assessment of the intelligence are conducted based on its nature, as outlined below：

i. Information intelligence related to information and communication security.

The content of information and communication security intelligence includes significant threat indicators, intelligence on Information Security vulnerabilities and attack methods, analysis reports of major security incidents, experience sharing on Information Security-related technologies or topics, and identification of potential system weaknesses or suspicious programs. These fall under the category of information intelligence related to information and communication security.

ii. Intrusion attack intelligence

The content of information and communication security intelligence includes specific web pages being attacked with clear evidence, inappropriate content on specific web pages with clear evidence, personal data leakage on specific web pages with clear evidence, specific systems being invaded with clear evidence, and specific systems engaging in network attack activities with clear evidence. These fall under the category of intrusion attack intelligence.

iii. Sensitive information intelligence

The content of information and communication security intelligence includes sensitive information such as names, birthdates, national identification numbers, passport numbers, characteristics, fingerprints, marital status, family details, education, occupation, medical history, healthcare, genetic information, health examinations, criminal records, contact information, financial status, social activities, and other directly or indirectly identifiable personal data. It also involves information related to individuals, legal entities, or groups' business secrets, or information concerning the operations of businesses. The intelligence may be publicly disclosed or provided, posing a threat to the rights or legitimate interests of public organizations, individuals, legal entities, or groups. Additionally, it may involve general official secrets, sensitive information, or national secrets. This falls under the category of sensitive information intelligence.

iv. Intelligence involving core business and core information and

communication systems.

The content of information and communication security intelligence includes internal core business information within the group, core information and communication systems, and operations related to critical infrastructure maintenance involving core business or core information and communication systems. This falls under the category of intelligence involving core business and core information and communication systems.

b. Response measures for Information Security incidents

After classifying and assessing information and communication security intelligence, the group should implement corresponding measures based on the nature of the intelligence. If necessary, adjustments to the control measures in the information and communication security maintenance plan may be made.

i. Information Security-related intelligence information

After the Information Security Promotion Team consolidates intelligence information, conduct risk assessment, and implement corresponding risk prevention mechanisms based on the controls outlined in the Information Security maintenance plan.

ii. Intrusion attack intelligence

Determine immediate danger by Information Security professionals; take immediate reporting and response measures if necessary. Implement corresponding risk protection measures according to the Information Security maintenance plan and notify relevant units for preventive actions.

iii. Sensitive intelligence information

For content involving personal data, trade secrets, general official secrets, sensitive information, or national secrets, exclusion measures such as masking or deletion should be taken. For example, in the case of personal data and trade secrets, specific sections or text should be masked or deleted, or de-identification methods should be employed.

iv. Intelligence information related to core business and core information communication systems.

The Information Security Promotion Team should assess whether intelligence information related to core business and core information communication systems has an impact on the overall operation of the group. Accordingly, implement corresponding risk management mechanisms based on

the Information Security maintenance plan.

L. Outsourcing Management of Information Systems or Services

When outsourcing the establishment, operation, or provision of information and communication systems or services within the group, consideration should be given to the expertise and experience of the entrusted party, the nature of the outsourcing project, and the Information Security requirements. Appropriate contractors should be selected, and their Information Security maintenance should be supervised.

a. Considerations for appointing contractors

1. The entrusted party should have well-established Information Security management measures or be verified by a third party regarding the relevant procedures and environment for handling entrusted business.
2. The entrusted party should have an adequate and appropriately qualified team, including Information Security professionals who have received proper training, possessed Information Security certifications, or had similar business experience.
3. The permissibility of sub-contracting by the entrusted party, the scope and entities allowed for sub-contracting, and the Information Security maintenance measures required for subcontractors in case of sub-contracting should be specified.

b. Considerations for monitoring the Information Security maintenance of the contractors.

1. In the execution of entrusted tasks, if the entrusted party violates relevant Information Security laws or becomes aware of Information Security incidents, they should promptly notify the contracting group and implement necessary remedial measures.
2. When the outsourcing relationship terminates or is dissolved, it should be ensured that the entrusted party returns, transfers, deletes, or destroys the data held in fulfillment of the outsourcing contract.
3. Other Information Security-related maintenance measures that the entrusted party should adopt.
4. When signing a contract with the entrusted party, review the confidentiality clauses in the contract and request business executives of the entrusted party

to sign a " Confidentiality Pledge for Outsourced Vendor Executives" and a " Confidentiality Agreement for Outsourced Vendor Executives."

5. The group should regularly or, upon awareness of potential Information Security incidents that may affect the entrusted business by the entrusted party, verify the execution status of the entrusted business through audits or other appropriate means. Audit items can refer to the "Outsourced Vendor Audit Checklist."

M. Information Security Education and Training.

a. Requirements for Information Security education and training

1. According to the Information Security level, the group, classified as level two, requires general users and supervisors to undergo a minimum of one hour of general Information Security education and training annually.

b. Method of conducting Information Security education and training

1. The responsible department should announce annually for colleagues to undergo physical or online learning, aiming to establish employee awareness of Information Security, enhance the group's Information Security standards. Additionally, relevant records of Information Security awareness promotion and education training should be retained, such as the "Information Security Awareness and Training Attendance Sheet."

2. The content of the group's Information Security awareness promotion and education training may include：

   (1) Information Security policy (including the content of the Information Security maintenance plan, management procedures, processes, requirements, personnel responsibilities, Information Security incident reporting procedures, etc.).

   (2) Legal provisions regarding Information Security.

   (3) Operational content related to Information Security.

   (4) Technical training related to Information Security.

3. When employees report for duty, they should be fully informed about the group's operational regulations related to Information Security and their importance.

4. The policy for Information Security education and training should apply

uniformly not only to employees within the group but also to external users.

N. Continuous improvement and performance management mechanism for the Information Security Maintenance Plan and its implementation.

a. Implementation of the Information Security Maintenance Plan

To implement this security maintenance plan and ensure the effective operation of Information Security management within the group, relevant units, when establishing documents, processes, procedures, or control measures at various levels, should align them with the group's Information Security policy, objectives, and the content of this security maintenance plan. Additionally, records of relevant implementation outcomes should be retained.

b. Audit mechanism for the implementation of the Information Security Maintenance Plan

i. Implementation of the internal audit mechanism

1. The Information Security Promotion Team should conduct internal audits regularly (at least once a year) or after significant system changes or organizational restructuring. This aims to verify whether personnel comply with this regulation and the management procedure requirements of the group, and to ensure the effective implementation and maintenance of the management system.

2. Internal audit operations can be conducted through self-assessment or on-site audits exchanged among different groups. The following explains these operational methods：

(1) Self-assessment: The Information Security Promotion Team assesses the implementation status based on the "Audit Self-Assessment Form," selects the appropriate audit results, and describes the findings in the comments section. When the audit result is non-compliant, the Information Security Promotion Team should propose improvement measures in the comments section and implement them.

3. Audit results should be reported to relevant management levels (including the Chief Information Security Officer), and relevant records of the audit process should be retained as evidence of the audit event.

c. Continuous improvement and performance management of the Information

Security Maintenance Plan

1. The group's Information Security Promotion Team should annually confirm the "Information Security Maintenance Plan" and the "Implementation of the Information Security Maintenance Plan" through announcements or meetings to ensure their ongoing appropriateness, suitability, and effectiveness.
2. If there are areas in the "Implementation of the Information Security Maintenance Plan" that require improvement, a "Performance Improvement Tracking Report" should be created. Relevant records should be retained as evidence for management review and execution.

O. Submission of the Implementation of the Information Security Maintenance Plans

In accordance with Article 12 of these regulations, the group shall submit the "Implementation of Information Security Maintenance Plans" within the specified timeframe, enabling an understanding of the annual implementation of Information Security plans within the group.

P. Relevant laws, procedures, and forms

a. Relevant laws and reference documents.

1. Information and Communication Security Management Act
2. Enforcement Rules of the Information and Communication Security Management Act
3. Classification Measures for Information and Communication Security Responsibility Levels
4. Information and Communication Security Incident Reporting and Response Measures
5. Measures for Information and Communication Security Information Sharing
6. Information Security Incident Reporting and Incident Response Management Procedure

b. Attachment Forms

F0219-1. Information Security Promotion Team Member Planning Explanation and Assignment Sheet

F0219-2. Information Security Confidentiality Agreement

F0219-3. Information Security Requirement Application Form

F0219-4. Inventory of Information and Communication System Assets

F0219-5. Asset Value Assessment Form

F0219-6. Likelihood and Impact Assessment Form

F0219-7. Threat Vulnerability Mapping Table

F0219-8. Risk Assessment Form

F0219-9. Risk Improvement Plan Form

F0219-10. Confidentiality Pledge for Outsourced Vendor Executives

F0219-11. Confidentiality Agreement for Outsourced Vendor Executives

F0219-12. Outsourced Vendor Audit Checklist

F0219-13. Information Security Awareness and Training Attendance Sheet

F0219-14. Audit Self-Assessment Form

F0219-15. Performance Improvement Tracking Report

F0219-16. Implementation of Information Security Maintenance Plan