

Notice

Information Technology Security Policy

Whereas I.C.C. International Public Company Limited (“Company”) has provided the use of information technology systems to facilitate, increase efficiency and effectiveness of the entire system's operations, to ensure that the use of services and provision of services can be carried out appropriately in accordance with business policies and to prevent problems that may arise from the improper use of information technology networks from users and various threats which may affect the Company's business systems.

Therefore, in order for the Company's information technology system to remain secure, complete and ready for use; the Information Technology Security Policy has been established as a guideline for implementation as follows:

1. Scope and Objectives

1.1 Scope

The Company defines the scope of information operations to establish clear standards and guidelines for data and information system management. The scope covers data management, technology systems, personnel, and all related processes from development, usage, maintenance, as well as prevention and risk management focusing on information systems that are secure, reliable, and ready for use, to be consistent with the goals of sustainable business development.

1.2 Objectives

- To protect data and information systems to ensure security
- Ensure continuous availability of the Company's information systems
- Build confidence among stakeholders in using the Company's information system services.
- To uphold the level of information system services that are secured in accordance with international standards and consistent with the Company's regulations and relevant laws.

2. Risk Management

The Company implements a comprehensive Information Technology Risk Management framework through a structured risk management plan. This plan identifies potential risks, defines assessment criteria, and outlines necessary improvements and mitigation strategies. The objective is to

minimize or appropriately manage risks in the development and operation of information systems, ensuring they are accurate, complete, timely, and fully operational.

Key risk factors include threats to confidentiality, integrity, and availability of data and information system assets. To effectively categorize and address risks, the Company classifies them into five levels which are critical, high, medium, low and very low.

3. Information Technology Security Management

The Company is committed to information security management to safeguard data and systems from potential threats. Our policies encompass the following key areas:

3.1 Personnel

- Enhance security awareness, knowledge, and skills among employees and stakeholders.
- Define roles and responsibilities, supported by relevant policies, manuals, and best practices.
- Conduct regular training and communicate security guidelines through official Company channels.
- Implement background checks, verify qualifications, review employment terms, and require confidentiality agreements during the hiring process.

3.2 Physical and Environmental Factors

- Implement access control measures for different areas, including general zones, critical locations, and the Company's Data Center.
- Deploy appropriate security systems, such as CCTV surveillance and access control mechanisms (e.g., key cards).
- Establish protocols to assess and safeguard critical equipment and data.
- Ensure security measures apply to all employees, users, and individuals involved in the Company's information systems.

3.3 Access Control and Information System Usage

- Implement identity verification processes and define appropriate access privileges.
- Encrypt sensitive data using secure standards for both storage and transmission.
- Protect information stored on Company computers, servers, and cloud systems.
- Manage user access through proper registration, authorization, revocation, and periodic reviews.
- Regulate the use of mobile devices to align with security standards.
- Safeguard personal data in compliance with legal and regulatory requirements.

3.4 Event Logging and Security Monitoring

- Deploy logging and monitoring systems to track activities within information systems.
- Record and analyze key events, including administrative actions, anomalies, and system errors.
- Secure log data against unauthorized modification, deletion, or access.
- Regularly analyze recorded data to detect potential threats and prevent security incidents that may impact the Company.

4. Data Management and Storage Media

The Company has implemented a structured data management system to ensure secure access and usage of information. This includes categorizing data confidentiality levels for both physical and electronic formats, as well as defining policies for storage media and document handling.

4.1 Data Management

To safeguard data and manage access appropriately, the Company categorizes information into five levels of confidentiality:

- **Public**
 - Information that can be released externally without affecting the Company.
 - **Examples:** Company website, public relations information, publicly available annual reports, job announcements, publicly available employee welfare information, press releases about the Company's products and services, documents used for presentation to customers or interested parties
- **Restricted / Internal Use**
 - Information intended for internal use that may be shared across departments with some restrictions.
 - **Examples:** Company's activity plans such as Internal seminar schedule, performance reports used in internal meetings, internal information technology system user manuals, internal announcements on employee benefits, employee rights, and details on expense reimbursement policies.
- **Restricted / Internal Use Only**
 - Information used within the Company for specific lines of work only and should not be disclosed to outsiders.

- **Examples:** Policies and operational manuals for each line of work, meeting reports of each line of work that have not been released to the public, list of employees, Internal contact information, training information, personnel development plans, and document approval system within the Company
- **Highly Confidential**
 - Sensitive information that could impact the Company if disclosed but is not as critical as "Restricted" data.
 - **Examples:** Business strategy plan that has not been released to the public, quarterly earnings report before release, information about key customers such as business contract agreements, details about employee salary structure, list of suppliers with price agreements and special terms.
- **Restricted**
 - Highly sensitive information that could cause severe financial, legal, or security risks if exposed.
 - **Examples:** Undisclosed merger or acquisition plans, high-level passwords for the Company's servers and main databases, undisclosed strategic or technological insights, senior executives' personal data such as ID card copies, income, assets, etc., and legal information under court proceedings

4.2 Storage Media Management

The Company enforces systematic management of storage media, covering data storage devices, critical documents, and operational records. This includes policies, IT security guidelines, operating procedures, system setup manuals, and official records.

4.3 Document and Information Management Process:

The Company has established procedures to ensure the secure handling of documents and information:

- **Document Registration & Approval:** New documents must be registered and approved by senior executives or authorized personnel before use.
- **Publishing & Revision Guidelines:** Documents are reviewed and updated regularly to maintain security and compliance.
- **Document Retention & Disposal:** Expired or obsolete documents are securely decommissioned and destroyed.

- **Security Classification:** Documents are assigned security levels based on their confidentiality.
- **Access Control:** Use security measures such as setting passwords and access rights to information systems.

These measures aim to ensure that the Company's data is protected and supports sustainable continuity business operations.

5. Data Backup and System Recovery

The Company has implemented a data backup and system recovery policy to ensure the restoration of critical data and systems in the event of unexpected incidents or disasters. The key operational guidelines are as follows:

5.1 Data Backup

- Perform regular backups using secure and reliable technologies.
- Implement both online and offline backup solutions to ensure quick and complete data recovery.
- Define backup guidelines and standards based on the data's level of importance.
- Restrict access to backup data to prevent unauthorized modifications, alterations, or deletions.

5.2 System Recovery

- Develop a comprehensive system recovery plan outlining roles, responsibilities, processes, and security measures.
- Ensure the recovery plan covers both data restoration and system recovery to resume normal operations.
- Conduct regular testing of the recovery plan to validate its effectiveness.
- Continuously update and refine recovery guidelines to align with evolving technologies and emerging risks.

These measures ensure business continuity, minimize operational disruptions, and enhance the Company's resilience against potential threats.

6. Management of Information Technology Assets and Information Capability

The Company has implemented policies for the efficient and secure management of IT assets and information capability to ensure sustainability and operational stability.

6.1 Management of Information Technology Assets

The Company manages various IT assets throughout their lifecycle, covering the following categories:

- Types of Assets under the Management
 - Data
 - Hardware
 - Software
 - Personal device (Bring Your Own Device: BYOD) used for work
 - Personnel
 - Services
 - Domains
 - Cloud and social media platforms
- Asset Management Measures
 - Implement controls to ensure appropriate asset usage throughout its lifecycle:
Procurement → Registration → Maintenance → Distribution → Disposal
 - Manage assets based on the confidentiality level of the data they contain.
 - Conduct regular asset reviews to maintain an up-to-date asset registry.
 - Mitigate risks associated with outdated technology that could cause hardware and software failures.
 - Define user responsibilities regarding IT asset usage.
 - Support long-term sustainable IT development.

6.2 Management of Information Capability

To ensure that IT resources remain efficient and sufficient, the Company has established the following management framework:

- Information Resources under the Management
 - Information technology infrastructure
 - Personnel

- Devices
- Technology
- Information service provider networks
- **Information Capability Management Measures**
 - Optimize the use of IT resources to maximize efficiency.
 - Align IT resources with Company needs and user requirements.
 - Ensure operational continuity, stability, and scalability.
 - Implement measures to maintain high-quality and sufficient IT resources.
 - Control to be in line with the budget allocation.
 - Regularly maintain and upgrade IT resources to ensure system security and reliability.

7. Procurement, Development and Maintenance of Information Systems

7.1 Procurement and Development of Information Systems

The Company is committed to procuring and developing information systems that effectively and securely meet business needs. To achieve this, policies are in place to control the installation process, ensuring that only authorized software with high-security standards is used.

7.2 Update and Maintenance of Information Systems

The Company regularly monitors, updates, and maintains software to prevent potential technical vulnerabilities. This ensures the information systems remain secure, stable, and continuously operational.

7.3 Information System Testing before Implementation

The Company prioritizes rigorous system testing before deployment, identifying and addressing vulnerabilities to mitigate risks to corporate data and systems. Compliance with this policy ensures that the Company's information systems remain robust, secure, and capable of supporting business growth and future changes.

8. Network and Communication Management

8.1 Network Security Measures

The Company enforces a strict policy on network and communication management to ensure maximum efficiency and security against various threats. This includes establishing appropriate usage guidelines and implementing security systems such as firewalls, antivirus programs, and intrusion prevention systems to prevent unauthorized access.

8.2 Network and Data Communication Access Control

The Company has established access controls for network systems via both wired and wireless networks, including external operations related to data transmission. These controls take into account the level of data importance and cover both internal and external departments to prevent unauthorized access to the Company's information systems and mitigate risks that could impact business operations.

8.3 Communication and Review of Measures

The Company emphasizes effective communication of network security measures to relevant parties to ensure proper understanding and compliance. These measures are periodically reviewed to maintain effectiveness and alignment with current circumstances.

9. Management of Services Provided by External Agencies

9.1 Quality Control and Safety of External Services

The Company has established policies to ensure that services provided by external agencies meet quality and safety standards in accordance with corporate requirements. This includes strict monitoring and review of the Service Level Agreement (SLA) to define service levels, emergency response measures, and regulatory compliance.

9.2 Evaluation and Monitoring of Service Performance

The Company regularly evaluates the efficiency of services provided by external agencies to ensure continuous improvement and their ability to meet corporate service needs effectively and securely. This process helps maintain service quality, data security, and system integrity related to external service provision.

9.3 Supervision and Change Management

The Company has established rules, regulations, criteria, and operational guidelines for monitoring, reviewing, and managing changes in service provision. Regular assessments of external service providers are conducted to control access to and usage of the Company's data and information systems, ensuring accuracy and security.

10. Change Management

10.1 Change Management Process in Information System and Business process

The Company is committed to managing changes in information systems and business processes in a structured and controlled manner to ensure that every change does not compromise system stability or security. This is achieved by defining a clear process that includes planning, testing, and monitoring the outcomes after implementation.

10.2 Control, Monitoring and Improvement of Change Process

The Company enforces strict control and monitoring of changes in information systems and business processes to ensure compliance with corporate standards and requirements. Continuous evaluation and process improvement are conducted to enhance efficiency and mitigate risks associated with future changes.

11. Operational Continuity Management and Information Security Incident Management

11.1 Operational Risk Planning and Prevention

The Company has established policies to ensure operational continuity by focusing on both risk prevention and recovery strategies. In the event of an emergency, these measures allow business operations to continue uninterrupted, even in unforeseen situations. The Company has developed detailed plans and procedures to handle emergencies that may impact operations, including natural disasters, system failures, or major technical incidents.

11.2 Information Security Incident Management

The Company has implemented comprehensive guidelines for managing information security incidents, covering responses to security threats, intrusion prevention, and system security breaches. These guidelines outline the roles and responsibilities of involved personnel, procedures for incident detection, reporting, analysis, evidence collection, resolution, and documentation. This ensures a rapid, effective, and systematic response to security incidents.

11.3 Monitoring, Review and Improvement of Process

The Company regularly monitors, reviews, and enhances its recovery plans, operational continuity strategies, and incident management procedures. Resources are prepared, and periodic drills are conducted to test response effectiveness. Lessons learned from past incidents are analyzed to develop preventive measures, ensuring uninterrupted business operations while minimizing the likelihood and impact of future incidents.

12. Evaluation, Report and Compliance

12.1 Evaluation and Report

The Company is committed to conducting inspections, evaluations, and reporting to the Risk Management Committee while ensuring operations align with the Information Security Policy. The Company regularly reviews and improves its policies, procedures, standards, work processes, documentation, and compliance with relevant laws and regulations. These reviews are conducted periodically or in response to significant changes, at least once a year, to ensure effective adaptation to advancements in information technology and environmental factors.

12.2 Compliance

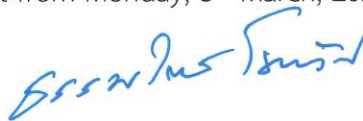
The Company continuously monitors and audits compliance with laws, regulations, contractual obligations related to information security, industry standards, and internal security requirements. This is achieved through communication with internal and external stakeholders, including business partners, customers, and service providers, to ensure awareness and adherence. Additionally, regular compliance reviews and audits are conducted to uphold the Company's policies and security framework.

13. Channels for disseminating policies and practices

To disseminate information security policies and practices to the Company's employees, stakeholders, customers, partners and relevant parties through the following channels:

- Websites such as intranet.icc.co.th, www.icc.co.th, investor.icc.co.th, and so on
- Applications such as ICCHR App
- Related documents and contracts

This Notice shall come into effect from Monday, 3rd March, 2025.



(Mr. Thamarat Chokwatana)

President