Information Security and Technology Policy

Pro Inside Public Company Limited

Edition: ISO/IEC 27001:2022

Effective date: 26 June 2026

Document owner: IT Department, Information Security Unit

Classification: Internal

Review cycle: At least once a year, or whenever there is a material change

Document Control

Revision history: v1.0 — Prepared in accordance with ISO/IEC 27001:2022

Distribution: Access is permitted only to employees/contractors who require it for their duties, and who must accept the terms of use of Pro Inside Public Company Limited information.

Table of Contents

Introduction 9
Executive Summary 9
1. Objectives and Scope 10
2. Relevant Standards, Laws and Acts 10
3. Terminology and Abbreviation 11
Components of Information Security 16
Information Security Management Structure 17
4. Role and Responsibility 17
4.1 Board / Governance Committee 17
4.2 Chief Executive Officer (CEO) and Top Executives of Subsidiaries 17
4.3 Information Security Committee (Working Group/Committee of the Group of Companies) 17
4.4 Information Security Officer 18
4.5 IT / System & Network Administrators 18
4.6 Information Asset Owner / System Owner 18
4.7 Application Owner / Development Team 18
4.8 Incident Response Team 19
4.9 Compliance/ Risk/ Legal/ DPO 19
4.10 Human Resources Management and Development Department (PD) 19
4.11 Procurement 19
4.12 All Users (Employees/ Contractors/ Third Parties) 19
4.13 Subsidiaries/Affiliates and the Security Coordinator of Each Unit 20
Information Security Policy 29
5. Organization Controls (Annex 5) 29
5.1. Policies for Information Security 29
5.2. Information Security Roles and Responsibilities 30
5.3. Segregation of Duties 30
5.4. Contact with Authorities 30
5.5. Contact with Special Interest Groups 30
5.6. Threat Intelligence 31
5.7. Information Security in Project Management 31

5.8. Inventory of Information and Other Associated Assets 31
5.8.1. Inventory of Assets 31
5.8.2. Acceptable Use for Information and Other Associated Assets 32
5.8.3. Handling of Assets 32
5.8.4. Return of Assets 32
5.8.5. Classification Information Control 33
5.8.6. Labeling of Information Control 35
5.8.7. Information Transfer 35
5.9. Access Control 36
5.10. User Access Management 36
5.10.1. User Registration and De-Registration 36
5.10.2. User Access Provisioning 37
5.10.3. Management of Privileged Access Right 37
5.10.4. Management of Secret Authentication Information of User 37
5.10.5. Review of User Access Rights 37
5.10.6. Removal or Adjustment of Access Rights 37
5.11. System and Application Access Control 37
5.11.1. Information Access Restriction 37
5.11.2. Use of Privileged Utility Programs 38
5.11.3. Access Control to Program Source Code 38
5.11.4. Access to Network and Network Services 39
5.11.5. Identity Management 42
5.11.6. Authentication Information 42
5.11.7. Use of Secret Authentication Information 43
5.12. Information Security in Supplier Relationships 43
5.12.1. Information Security Policy for Supplier Relationships 43

5.12.2. Control of Access by External Service Providers (Third Party) 44

5.12.3. Assessing Security within Supplier Agreements 44

5.12.4. Information and Communication Technology Supply Chain 45

5.12.5. Supplier service delivery management 45

5.12.6. Information Security for using Cloud Services 46

5.13. Management of Information Security Incidents and Improvements 46

5.13.1. Other Acts Prohibited by the Company 46

5.13.2. Reporting information security weaknesses 48

5.13.3. Assessment of and decision on information security events 48

5.13.4. Response to information security incidents 49

5.13.5. Learning from information security incidents 50

5.14. Collection of Evidence 50

5.15. Information security during disruption 51

5.15.1. Information Security Aspects of Business Continuity Management 51

5.15.2. Information security continuity 51

5.15.3. Implementing information security continuity 51

5.16. Redundancies 52

5.16.1. Availability of information processing facilities 52

5.16.2. ICT readiness for business continuity 53

5.17. Legal, statutory, regulatory and contractual requirements 53

5.17.1. Compliance with Legal and Contractual Requirements 53

5.18. Intellectual Property Rights 54

5.18.1. Protection of Records 55

5.18.2. Privacy and protection of personally identifiable information 55

5.18.3. Protection of Organizational Records 55

5.18.4. Regulation of cryptographic controls 55

5.18.5. Prevention of Misuse of Information Processing Facilities 55

5.18.6. Independent Review of Information Security 56

5.18.7. Compliance with policies, rules and Security Standards for information security 56

5.18.8. Technical Compliance Review 56

5.18.9. Document Operating Procedures 56

6. People Control Annex 6 56

6.1. Prior to Employment 56

6.1.1. Screening 56

6.1.2. Terms and Conditions of Employment 57

6.2. During employment 58

6.2.1. Information Security Awareness, Education and Training 58

6.2.2. Disciplinary process 58

6.3. Responsibilities after Termination or Change of Employment 58

6.3.1. Termination or change of employment responsibilities 58

6.3.2. Confidentiality or Non-Disclosure Agreements 59

6.3.3. Teleworking 59

6.3.4. Information Security Event Reporting 60

7. Physical Controls Annex 7 60

7.1 Physical and Environmental Security 60

7.2. Secure areas 61

7.2.1. Physical Entry Controls 61

7.2.2. Securing Offices, Rooms and Facilities 62

7.2.3. Protecting against external and environmental threats 62

7.2.4. Working in secure areas 63

7.2.5. Delivery and loading areas 63

7.3. Equipment Security 63

7.3.1. Equipment siting and protection 63

7.3.2. Supporting Utilities 64

7.3.3. Cabling Security 64

7.3.4. Equipment Maintenance 64

7.3.5. Removal of Assets 65

7.3.6. Security of Equipment and Assets Off Premises 65

7.3.7. Clear Desk and Clear Screen Policy 65

8. Technological Control (Annex 8) 65

8.1. Mobile Device Policy 65

8.1.1. Unattended User Equipment 66

8.1.2. Privileged Access Rights 67

8.1.3. Information Access Restriction 67

8.1.4. Access Control to Program Source Code 67

8.1.5. Secure Authentication 68

8.1.6. Capacity Management 68

8.1.7 Separation of Development, Testing and Operational Environments 68

8.2 Protection from Malware 68

8.2.1 Control Against Malware 68

8.2.2. Management of Technical Vulnerabilities 69

8.2.3. Technical Compliance Review 69

8.2.4. Configuration Management 70

8.2.5. Information Deletion Control 70

8.2.6. Data Masking 70

8.2.7. Data Leakage Prevention Control 71

8.2.8. Information Backup 71

8.2.9. Redundancies 72

8.3. Logging and Monitoring 72

8.3.1. Event Logging 72

8.3.2. Protection of Log Information 72

8.3.3. Administrator and Operator Logs 75

8.3.4. Monitoring Activities 75

8.3.5. Clock Synchronization 75

8.3.6. Control of Operational Software 76

8.3.7. Restrictions on Software Installation 76

8.4. Network Security 77

8.4.1. Network Control 77

8.4.2. Security of Network Services 78

8.4.3. Segregation in Networks 78

8.4.4. Web Filtering 79

8.5. Use of Cryptography 80

8.5.1. Cryptographic Controls 80

8.5.2. Key Management 81

8.6. Security in Development and Support Processes 81

8.6.1. Secure Development Policy 81

8.6.2. System Change Control Procedures 81

8.6.3. Technical Review of Applications after Operating Platform Changes 81

8.6.4. Restrictions on Changes to Software Packages 81

8.6.5. Secure System Engineering Principles 82

8.6.6. Secure Development Environment 82

8.6.7. Outsourced Development 82

8.7.8. System Security Testing 83

8.7.9. System Acceptance Testing 84

8.8. Test Data 84

8.8.1. Protection of Test Data 84

8.9. Change Management 85

8.9.1. Change Management Policy 85

8.9.2. System Change Control Procedures 85

8.9.3. Technical Review of Applications After Operating Platform Changes 86

8.9.4. Restrictions on Changes to Software Packages 86

9. Legal Compliance and Regulatory Requirements 86

10. Regulations and Penalties 86

Conclusion 88

Introduction

Executive Summary

In today's digital era, data and technology are strategic assets that drive the success of Pro Inside Public Company Limited. Information and technology security is therefore a vital foundation for building the confidence of customers, partners, shareholders and society. This Information Security and Technology Policy have been prepared to set out a clear direction, standards and practices covering data protection, risk management, business continuity, personal data privacy, the security of cloud systems, networks, endpoint devices and applications, as well as the management of external service providers.

The management of Pro Inside Public Company Limited affirms its commitment to the following:

- Comply with all applicable laws and requirements, including the Personal Data Protection Act (PDPA), the computer-Related Crime Act, and appropriate international practices (e.g. ISO/IEC 27001).
- Manage cyber risks systematically, based on risk management principles, with emphasis on business impact and continuity of service.
- Invest in and support the resources, personnel, processes and technology necessary to strengthen readiness to prevent, detect, respond to and recover from security incidents.
- Build a security culture at every level, promoting regular learning and training so that everyone is aware and able to comply effectively.
- Continually review and improve policies, measures and controls through periodic assessments, testing and independent audits.

Security is a shared responsibility of everyone in the Company. All employees and relevant parties are therefore requested to:

- Study, understand and strictly comply with the Company's policies and practices.
- Protect information according to its level of sensitivity, use strong authentication (e.g. MFA) and manage passwords securely.
- Be vigilant against social engineering threats and e-mail phishing, and report incidents or anomalies immediately through the designated channels.
- Follow the procurement and external service provider risk management processes to ensure that the supply chain is secure.
- Support testing, business continuity/disaster recovery plans and continual improvement.

This policy applies to employees, temporary staff, consultants, contractors and all business partners who access the information or systems of Pro Inside Public Company Limited and should be reviewed at least once a year or whenever there is a significant change in risk, technology or regulatory requirements.

1. Objectives and Scope

To ensure that the Company's information technology systems are used by users appropriately, efficiently and securely, and that system operations can continue without interruption; to prevent problems that may arise from improper use of information technology systems and from threats in various forms that affect business operations; and to reduce risks that are likely to occur, the Company establishes Standards, Guidelines and Procedures covering information technology system security and the prevention of various threats, with the following objectives:

1.1 The establishment of information security policies and practices to create confidence and security in the use of the Company's information technology systems or computer networks, enabling operations to be conducted with the greatest efficiency and effectiveness.

1.2 To define the scope of information technology system security management with reference to international standards, with continual improvement of the information security policies and practices; and further, to apply the unit's risk assessment framework to the management of information technology work using the Information Security framework, namely Confidentiality (C), Integrity (I) and Availability (A).

1.3 This policy shall be disseminated against employees at all levels, and all employees shall accept and strictly comply with this policy.

1.4 To establish standards, guidelines and methods of practice so that management, employees, System Administrators and third parties working for the Company are aware of the importance of maintaining security in the use of the Company's information technology systems in their operations and comply with them strictly.

1.5 This policy shall be reviewed and evaluated periodically once per year.

1.6 This policy operates within the framework of the personal data protection process promulgated on 1 June B.E. 2565 (2022).

2. Relevant Standards, Laws and Acts

2.1 Computer-Related Crime Act B.E. 2550 (2007) and its amendment B.E. 2560 (2017): Defines offences and penalties relating to unauthorized access to data, interference with computer systems, dissemination of false information, data forgery, and causing damage to public infrastructure.

2.2 Electronic Transactions Act B.E. 2544 (2001) and its amendments: Gives legal recognition to electronic data and electronic signatures, making them binding in the same way as paper documents and handwritten signatures, to support online transactions.

2.3 Personal Data Protection Act B.E. 2562 (2019) – PDPA: Sets out the rules for the collection, use or disclosure of personal data to protect the rights of data subjects.

2.4 Cybersecurity Act B.E. 2562 (2019): Sets out measures and a framework for dealing with cyber threats and for maintaining the security of Critical Information Infrastructure (CII).

2.5 Emergency Decree on Electronic Meetings B.E. 2563 (2020): Recognizes meetings held via electronic media as having the same legal effect as ordinary meetings.

2.6 Copyright Act: Protects creators as soon as a work is created (no registration required), granting exclusive rights to reproduce, adapt and publish works such as literary works, artistic works, music, films, computer programs, and others.

2.7 ISO/IEC 27001: The globally recognized standard for Information Security Management Systems (ISMS), emphasizing the principles of Confidentiality, Integrity, and Availability (CIA Triad).

2.8 NIST Cybersecurity Framework (CSF): A framework of the National Institute of Standards and Technology (NIST) of the United States, providing best-practice guidance for managing cyber risk.

2.9 PCI DSS: The data security standard for the payment industry (Payment Card Industry Data Security Standard).

2.10 ISO/IEC 20000: (IT Service Management – ITSM) For managing IT services systematically and efficiently, e.g., Incident Management, Problem Management and Service Level Management.

2.11 ISO/IEC 27701: An extension of ISO 27001 for Privacy Information Management.

2.12 ITIL (Information Technology Infrastructure Library): A Best Practice framework for IT service management, which can be used together with ISO 20000.

3. Terminology and Abbreviation

- **Company** means Pro Inside Public Company Limited.
- **Employee, worker, and user** mean employees engaged under any type of employment to work for Pro Inside Public Company Limited, e.g., permanent employees, contract employees, temporary employees, and employees engaged for a period, including management at all levels employed by the Company.
- **System or computer system** means all types of tools, all types of servers and computer equipment, both wired and wireless, and everything in the equipment and various recording media used to transmit data via the Internet (outside the Company), extranet (within trusted networks connected to the Company) and intranet (within the Company), including all electronic equipment and telecommunications equipment used in a manner similar to

computers. This also includes items that are assets of the Company and of the SKY ICT group of companies, items belonging to co-workers or partners, and items belonging to vendors that are purchased, installed and located on the Company's premises, regardless of the condition of such items or equipment.

- **Data or computer data** means electronic, electrical, audio or any other type of signal that can be changed or converted to have meaning understandable by humans, such as text, still images, moving images, sound or other forms that can be used for communication between people using electronic devices or computer equipment to send messages from one place to another, or be stored in other tools, and can be reused temporarily or permanently.
- **Access** means entering premises, electronic or physical use, including obtaining knowledge of data.
- Access to or control the use of information: the inspection, approval and assignment of rights, or the authorization of users to access or use networks or information systems, both electronically and physically, and the revocation or cancellation of access rights.
- **Access control** means the authorization, assignment of rights, modification, revocation or cancellation of access rights.
- **Capacity Management** means the management of resources and the determination of the capacity of staff, operational plans, and others.
- **Change Management** means the process of controlling changes to information systems or work systems, where such changes affect Hardware, System Software, Application Software, Network System, etc.
- **Risk assessment** means the entire process of analyzing and evaluating risks.
- **Internal Use data group** means information used only within the Company. It may be disseminated within the Company but shall not be disclosed to third parties unless approved in writing by management at the level of department/unit manager of the data-owning unit or above, and a Non-disclosure Agreement shall be signed, unless such disclosure is made under authority recognized by law.
- **Confidential data group** means information which, if disclosed in whole or in part, would cause damage to the Company. Only authorized people may access it, and it shall not be disclosed to third parties unless approved in writing by the manager of the data-owning

department or above, and a Non-disclosure Agreement shall be signed, unless such disclosure is made under authority recognized by law.

- **Strictly Confidential data group (Confidential)** means information which, if disclosed as a whole or in part, would cause serious damage to the interests of the State. Only authorized people may access it, and it shall not be disclosed to third parties unless approved in writing by the manager of the data-owning department or above, and a Non-disclosure Agreement shall be signed, unless such disclosure is made under authority recognized by law.
- **Secret data group (Highly Confidential)** means confidential information which, if disclosed in whole or in part, would cause the most serious damage to the interests of the State. Only authorized persons may access it, and it shall not be disclosed to third parties unless approved in writing by the Chief Information Officer (CIO), and a Non-disclosure Agreement shall be signed, unless such disclosure is made under authority recognized by law.
- **Public data group** means information that is open and may be disseminated to the public.
- **Data** means anything that conveys meaning about a matter of fact, whether such meaning is conveyed by the nature of the thing itself or by any means, and whether it is in the form of a CD, DVD, Hard Disk, Thumb drive, document, report file, book, map, diagram, drawing, photograph, computer recording, or any other method that enables the recorded content to be displayed.
- **Information Security** means the preservation of Confidentiality, Integrity and Availability of information, as well as other properties, namely Authenticity, Accountability, Non-Repudiation and Reliability.
- **Business Continuity Management (BCM)** means the approach to managing the business continuously when the Company is in crisis and has various emergencies, ensuring that the Company's critical operational procedures and information systems are covered by an appropriate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
- **Information Owner** means the person responsible for the Company's data, including the supervisor of that data owner. The data owner is the person who is responsible for the data or who is directly affected if the data is lost.
- **System Owner** means the person responsible for using, looking after and maintaining, or improving work systems used in the Company.

- **Interns and trainee students** mean university and college students whom the Company permits to undertake work experience for a specified period.
- **Application** means a type of program created for specific use.
- **Information System Workspaces** means areas in which the Company permits information systems to be used, divided into:
    - **Secure Area**: an area with access control and protection systems against various threats.
    - **System Administrator / Operator Area**: an area used by system administration staff to carry out the administration of the Company's information systems.
    - **Working Area**: general workrooms and meeting rooms, e.g. general working areas of the Company's employees.
    - **General Area**: an area used for receiving people who contact the Company.
- **Network System** means a system that can be used to communicate or transmit data between computer systems, such as LAN (Local Area Network), WLAN (Wireless LAN), Intranet, and systems, etc.
- **Wireless LAN (WLAN)** means a network system connecting computer systems, including communication via alternative communication channels.
- **Information System** means a work system that uses technology to help create information that can be used for planning, management, service support, development and control of communications, consisting of computer technology and telecommunications technology, such as Computer System, Network System, Software, Data and Information, etc.
- **Intranet** means a network system that can be accessed only by users within the Company, for the purpose of communication and exchange of data and information within the Company.
- **Internet** means a network system that connects the Company's computer systems to computer systems around the world.
- **LAN** means a network system that connects computers together within a limited distance, such as within the same building or the same area where cables can be run directly between them.

- **Information Security Incident** means an undesirable or unexpected security situation that is likely to cause the Company's systems to be intruded upon or attacked, and security to be threatened.
- **Information** means facts derived from data that have been processed and organized, which may be in the form of numbers, text or graphics, into a system that users can easily understand and use for management, planning, decision-making and other purposes.
- **User rights**: rights and duties according to Role relating to the Company's information systems are as follows:
    - **General user rights** mean the board of directors, directors, deputy directors, department managers, employees, staff and people using the Company's basic information systems. Users shall obtain permission from the department/unit manager or above, using the approval request form prescribed by the Company.
    - **Privileged rights** mean rights additionally assigned by the supervisor on a special basis. Users shall be assigned such rights by the supervisor on a case-by-case basis.
- **Social media** means online communities in which Internet users can exchange experiences with one another using various media as the vehicle for conversation. Social media is classified into several types, namely:
    - **Publish**, e.g. Wikipedia, WordPress, Pantip, etc.
    - **Discuss/SMS/Instant Messaging**, e.g. Line, Skype, Facebook Messenger, etc.
    - **Social Network**, e.g. Facebook, LinkedIn, Instagram, Twitter, etc.
    - **Online Video**, e.g. YouTube, Netflix, TikTok, etc.
    - **Photo Sharing**, e.g. Flickr, Photobucket, etc.
- **External agency / external service provider / third party** means an external service provider (Third Party) or outside person who uses the Company's information systems occasionally or under contract.
- **Information security event**: an occurrence of an event or a state of a service or network indicating a possible breach of the information security policy or failure of protective measures, or a previously unknown situation that may be relevant to security.

- **Mobile Device**: a small portable processing device that can be operated with one hand, with touch-based input not requiring a Keyboard, and able to connect to wireless networks and telephone networks, e.g. Smartphone, Tablet, etc.
- **Computing Device**: a device with a processing unit, memory, data storage, network connectivity, input unit and display unit, namely:
    - Desktop computers, e.g. Desktop Computer, etc.
    - Portable computers, e.g. Notebook, Netbook, etc.

Components of Information Security



The diagram above shows that the information security policy is a document whose content refers to the goals, objectives and values of the Company, which primarily affect the Company's image. Therefore, applying various methods in line with the policy and business direction is something that must be put into practice. In addition, legal rules and regulations play an important part in drafting this information and data security policy, such as data protection laws and electronic document laws already in force. Finally, defining the roles, duties and responsibilities of employees in each relevant unit is an important element in enabling employees to work in line with the defined objectives and goals.

Information Security Management Structure

All policies, regulations and procedures are maintained as documents approved and accepted by management, and the Company's employees are informed of the existence of the policy. From the perspective of the policy, it is important to every department and to all departments throughout the Company. Therefore, Company information provided to employees and information under the responsibility and actions of employees, the safeguarding of information, the systems used to process information, and even the methods used to transfer information, shall all be subject to review.

4. Role and Responsibility

To support the VISION and MISSION of the group of companies in developing smart technology solutions for the private and public sectors, the group of companies defines the roles and responsibilities for information security and information technology systems as follows:

4.1 Board / Governance Committee

- Approve and oversee the policy direction for information security of the group of companies.
- Ensure that cyber risk is managed at the enterprise level and monitor significant risk issues.
- Acknowledge reports of Major Incidents of information security and the results of reviews/improvements of key measures.

4.2 Chief Executive Officer (CEO) and Top Executives of Subsidiaries

- Provide sufficient resources (people/budget/tools) for security operations.
- Appoint people responsible for information security and define their authority and duties.
- Approve Risk Acceptance/Exception at the levels prescribed by the regulations of the group of companies.

4.3 Information Security Committee (Working Group/Committee of the Group of Companies)

- Set the security goals, work plans and indicators (KPI/KRI) of the group of companies.
- Consider and prioritize risk issues/security projects.
- Review significant incidents and significant vulnerabilities and follow up on the closure of outstanding issues.
- Pursuant to Announcement No. 2568/06-1 appointing the Information Security and Technology Services Management System (ISTS) Committee, dated "1 June 2025".

4.4 Information Security Officer

- Prepare, maintain and review security policies/standards/procedures to keep them up to date.
- Provide advice on risk management, data classification and the definition of controls.
- Oversee key processes such as Vulnerability Management, Incident Response, Security Awareness and Access Control (from a policy/governance perspective).
- Report on the status of risks, significant incidents and policy compliance to the relevant management/committees.
- Coordinate with external parties (e.g. customers, government agencies, service providers) where security incidents are concerned.

4.5 IT / System & Network Administrators

- Implement technical controls in accordance with the policy, such as security configuration (hardening), patch management, backup, logging, network segregation and rights management.
- Follow the Change Management/CAB process and prepare evidence of changes that affect security.
- Support the verification/retest of vulnerabilities and the collection of evidence when abnormal events occur.

4.6 Information Asset Owner / System Owner

- Be responsible for determining the criticality of systems/data and approving access rights based on the need-to-know/least privilege principle, as determined by the Company.
- Be responsible for ensuring that systems under their care comply with the policy, including remediation of vulnerabilities within the defined SLA.
- Approve/jointly consider remediation plans, residual risks and Exceptions, together with compensating controls as prescribed.

4.7 Application Owner / Development Team

- Develop and maintain software in accordance with Secure SDLC practices (e.g. management of vulnerabilities in code/libraries/configurations).
- Remediate vulnerabilities in applications/components (dependencies) and deliver patches/fixed versions in accordance with the SLA.

- Record and review changes through the Change Management process as prescribed.

4.8 Incident Response Team

- Monitor, detect, analyze and coordinate the response to information security incidents.
- Carry out containment together with IT/system owners and prepare incident reports/lessons learned.
- Coordinate incident communication through the chain of command and in accordance with the organization's communication plan.

4.9 Compliance/ Risk/ Legal/ DPO

- Ensure that operations comply with relevant legal/contractual/standard requirements.
- Support impact assessments and the handling of incidents involving personal data in accordance with organizational procedures.
- Provide advice on requirements for evidence retention and notification to authorities/contracting parties (subject to the relevant conditions).

4.10 Human Resources Management and Development Department (PD)

- Apply the policy direction to improve and define guidelines according to conditions and methods, and to define security in personnel processes (e.g. Onboarding/Offboarding, policy acceptance, disciplinary measures).
- Support communication and security awareness training for employees/contractors.

4.11 Procurement

- Define security requirements in contracts/procurement (e.g. SLA, confidentiality, incident notification, right to audit).
- Monitor the risk assessment and compliance of service providers/business partners.

4.12 All Users (Employees/ Contractors/ Third Parties)

- Comply with the relevant policies and measures (e.g. password use, MFA, information handling, e-mail/Internet use, reporting of phishing e-mails).
- Report security incidents/anomalies immediately through the channels designated by the Company.
- Maintain the confidentiality of the information and assets of the group of companies and not take any action that violates the policy or the law.

4.13 Subsidiaries/Affiliates and the Security Coordinator of Each Unit

Implement this policy and the subordinate documents (standards/procedures) of the group of companies.

- Appoint a Security Focal Point to coordinate with the Cybersecurity unit of the group of companies.
- Report on the status of risks, incidents and performance against the SLA/requirements of the group of companies at the prescribed intervals.

Rights, Duties and Responsibilities

"Top Executive": Duties and Responsibilities

- In the event that a computer system or information is damaged, or any harm occurs to any person, due to a deficiency, negligence or violation of the information security policy, the senior executive assigned responsibility for the information of [the Company] shall be accountable for the risk, damage or harm that occurs, and shall have the authority to establish a committee to investigate the facts.

Rights

- May assign any classification level to data and information classified by the Company that are under their line of command.
- May access and use data and information of all classification levels under their line of command.
- May order the granting, revocation and suspension of users' rights to access or control the use of information of all classification levels under their line of command.
- May delegate authority in writing to subordinates to order the granting, revocation and suspension of users' rights to access or control the use of information of all classification levels under their line of command.
- May appoint "officers" to act as system administrators for information system work under their line of command.
- May permit external agencies to work on the Company's information systems.
- May define and classify the information system workspaces of [the Company] under their line of command.

- May define users' rights to enter and leave information system workspaces under their line of command and shall ensure that those who have such entry and exit rights strictly comply with the policies, rules and regulations relating to the Company's information systems as prescribed.

"Senior Executive": Duties and Responsibilities

- In the event that a computer system or information is damaged, or any harm occurs to the Company or to any person, due to a deficiency, negligence or violation of the information security policy, the senior executive assigned responsibility for the Company's information shall be accountable for the risk, damage or harm that occurs, and shall have the authority to establish a committee to investigate the facts.
- Has a duty to notify the unit responsible for information system security and the policy, so that it is informed and can compile information concerning:
- The assignment or change of rights of users under their line of command.
- The definition or change of information system workspaces under their line of command.
- The assignment or change of the classification level of data under their line of command.

Rights

- May assign any classification level to data and information classified by the Company that are under their line of command.
- May propose to the senior executive for consideration and instruction that resulting data or information arising from the processing of data or information originating from the line of command — namely results from processing data or information from multiple units, or with differing classification levels — be assigned an appropriate classification level.
- May access and use data and information of all classification levels under their line of command.
- May access and use other classified data and information about the Company to the extent permitted by the senior executive.
- May order, grant, revoke and suspend users' rights to access or control the use of classified information under their line of command.
- May propose to the senior executive to request permission for external agencies to work on the Company's information systems under their line of command.

- May define and classify the Company's information system workspaces under their line of command.
    - May define users' rights to enter and leave the Company's information system workspaces under their line of command and has the duty to ensure that those who have such entry and exit rights strictly comply with the policies, rules and regulations relating to the Company's information systems.

"Management": Duties and Responsibilities

- Supervise subordinates to ensure strict compliance with the information security policy and practices and approve and support resources.
- Control, oversee and be responsible for the information technology equipment of the unit.

Rights

- May access and use data and information assigned the security classification "Confidential" only where it falls under their line of command.
- May access and use data and information assigned the security classification "Highly Confidential" only to the extent permitted by "senior management", subject to the approval of the "middle management" who owns the information system.
- May permit persons or users to borrow information technology equipment under their responsibility.

"System Administrator" Duties and Responsibilities

- Has no right to open and read the private e-mail or private communications (e.g. Gmail, Outlook, LINE) of "users", except where used in an investigation of improper use of the system or infringement of the rights of others, or where requested by an external agency pursuant to a court order or by law.
- Has no right to open, read or use data and information assigned a security classification, except where written authorization has been granted by the management member who is empowered to authorize access to, or control the use of, that classified information.
- Shall notify users in advance of the date and time at which the system must be shut down for maintenance, improvement or change, resulting in a suspension of service for a period. In an emergency, the system administrator has the right to shut down the system immediately and shall endeavor to allow users to save their data completely before shutting down the system and shall prepare a report to inform the supervisor.

- Shall maintain, inspect, correct and propose improvements to the information systems and related procedures so that the systems remain in good working order, stable, secure and efficient always.
- Shall follow up on and instruct users and update the user database so that it is always accurate and current and shall delete from the database the user accounts of persons whose right to use the system has ended.
- Shall keep track of news, threat conditions and vulnerabilities of information systems, and shall regularly improve and maintain the systems to reduce the risk of intrusion.
- Should we obtain permission from the supervisor when cooperating with the unit responsible for information system security in assessing, auditing, testing and identifying weaknesses and vulnerabilities related to the security of information systems and should we remediate them promptly.
- Shall immediately notify the unit responsible for information system security, and report to supervisors through the chain of command, where it is detected, reported by users, or suspected that an information system under their direct responsibility, or any other related system of the Company, has suffered a security breach.

Rights

- May terminate the operation of an information system found to be a threat to security or to place an unnecessary burden on the Company's information systems without prior notice, in emergencies only, and shall investigate the cause and origin of such threat or burden and report to the supervisor responsible for the system.
- May terminate the operation of an information system that has been put into use without authorization from the Company, without prior notice, and shall investigate the cause and origin of that system and report to the supervisor.
- May restrict or suspend the rights of users who use the system improperly and notify the Company's management to appoint a committee to investigate or impose penalties as appropriate.

"Information Owner" Duties and Responsibilities

- Determine the security classification and access rights.
- Review the security classification level of data to ensure that it still meets operational requirements and is appropriate and consistent with that security level.

- Ensure that data is correctly and appropriately identified or marked with the security level at which it has been classified, regardless of its form or medium.
- Establish backup requirements and ensure that security breaches are handled appropriately.

Rights

- Approve and review to ensure that users' rights are correct and appropriate.
- Assign security classification levels to data.
- Define the security baseline for access to the unit's data.

"Application Owner" Duties and Responsibilities

- Ensure that the application functions correctly and consistently in accordance with requirements.
- Control and oversee the security of access to the application and the security of data.
- Approve, review and certify system access rights appropriate to the level of importance of the data.
- Establish requirements for the backup of the application's data and Source Code.
- Act or ensure that security breaches are handled appropriately.

Rights

- May delegate the above duties and responsibilities to other appropriate people, but the application owner shall remain fully accountable for the application.

"Users" Duties and Responsibilities

- The Company's computer equipment and network systems are provided for use in the Company's business only, except where the user has been granted specific permission by management.
- Shall help protect all equipment from damage. In the event of damage from accidents or any hazards, the user shall immediately report to the system administrator and the supervisor.
- When requesting the use of equipment and systems, the user shall be able to present a valid identification card if requested by the system administrator.
- Should use network resources efficiently, e.g. not downloading large files unnecessarily, not sending or forwarding chain e-mails, etc.

- For proper system administration, users shall provide correct personal identification information for the opening of user accounts (User ID or Login Account).
- Shall be responsible for setting a secure password in accordance with the Password Management Policy.
- Should we under no circumstances allow others to use the computer system through their own user account; otherwise, the user may be subject to disciplinary action and shall be responsible for any resulting problems, such as copyright infringement or the storage of illegal data, etc.
- Shall immediately report to the system administrator and the supervisor where it is detected or suspected that their own or another person's user account has been used without authorization or misused, and where any behavior violating the security of the system is observed.
- Shall protect data and information assigned a security classification from disclosure to others.
- Shall not intrude into information system areas without authorization.
- Shall use the system lawfully, without infringing the rights of, or causing trouble or damage to, other people or companies.
- Shall not install or operate network services on the Company's machines for personal purposes.
- Shall return the Company's assets relating to the performance of their duties immediately upon leaving their position, including equipment, information systems, data and copies of data, keys, identification cards, entry/exit passes, etc.
- Shall immediately report to the system administrator and the supervisor in the event of the relocation or removal of information system equipment.
- Shall comply with the Company's Standards, Guidelines and Procedures relating to information security.
- Users are prohibited from installing programs or devices on the Company's machines before obtaining approval from the unit responsible for the information system network, in order to prevent copyright issues and other problems that may arise after installation, such as installing an Access Point on one's own which then allows the network to be breached, or causes the spread of viruses and other threats, etc. [The unit] controls and oversees the security of access to applications and the security of data.

- If a deficiency in the security system is found, or anyone is suspected of acting suspiciously, the user shall report it to the system administrator immediately.
- Shall cooperate with the officers assigned to investigate incidents relating to the security of GISTDA (สทอภ.).

Rights

- May access information that is not data or information assigned to a security classification by the Company, except where written authorization has been granted by the management who is powered to authorize access to, or control the use of, that classified information.
- Violations may result in disciplines prescribed by Company regulations, and all users shall be unconditionally liable in accordance with the regulations.

"Unit Responsible for Information System Security" Duties and Responsibilities

- Consider the details of violations or breaches of information system security regulations and policies. Where the violation is serious, or where the violation has caused damage to the Company or to any person, a memorandum reporting the policy violation shall be prepared and submitted to management.
- Where the intent of a breach or violation is unclear, the violator shall be warned and explained the correct practice. If the violation is repeated, a review committee shall be appointed, and the act shall be reported immediately to senior management and the relevant supervisors, so that an investigation is conducted and disciplinary action is taken according to the severity of the impact of the breach or violation of such regulations.
- Prevent and resolve problems immediately to ensure that such breaches or violations do not escalate into major problems.
- Organize training to promote users' awareness of information security.
- Provide technical advice on the security of information systems.
- Plan the control of information security systems and warnings, including analyzing ways to remediate weaknesses in information systems.
- Investigate any events that do not comply with the information security policy.
- Liaise and coordinate to build security cooperation between companies.

- Compile names and contact information for other agencies, such as the Royal Thai Police, the National Security Council, the Thailand Computer Emergency Response Team (ThaiCERT), etc., for use in security liaison and coordination when necessary.

Rights

- Define the approval process for the use of new information systems and enforce the use of this process.
- Any legal action shall be undertaken with the assistance of the unit responsible for legal affairs and the Company's representatives, and the conduct of any litigation involving the Company shall be the duty solely of designated management-level officers.

"Unit Responsible for the Information System Network" Duties and Responsibilities

- Develop, install, inspect, improve, repair and maintain equipment, and manage IT Infrastructure equipment systems for all units.
- Administer all computer network systems used within the Company (Network Administration), and control direct connections to the Internet through other channels such as Dial-up Modems, as well as control network connections from outside, such as remote access to computers, the use of VPN, etc.
- Be responsible for procuring and controlling the use of the Corporate Antivirus; prepare manuals and information relating to the Corporate Antivirus; compile statistics, graphs and usage results; and permit or restrict the use by users.
- Be responsible for maintaining and closing vulnerabilities in the Corporate Antivirus system, keeping the Corporate Antivirus Virus Signatures up to date, and proposing the budget through the responsible unit.
- Be responsible for information system security; increase or decrease the number of Corporate Antivirus licenses; permit or restrict the use by users; and carry out related actions.
- Be responsible for creating and updating the content of the Company's website.
- Control the installation of programs or devices on computers.
- Be responsible, jointly with the system administrator, for auditing software to prevent breaches of agreements, and to find ways to protect the software used for system assessment so that it is not misused, and to protect sensitive data produced as a result of audits by such software.

- Compile records of the Company's information system assets, including the Configuration settings of network devices, for efficient management of the Company's information systems.
- Provide advice and act as consultant in considering the details of violations or breaches of the Company's information system security regulations and policies and resolve such problems.
- Control information security systems and warnings, including analyzing ways to remediate weaknesses in information systems.
- Define and control the Backup & Recovery of the Company's information systems.
- Control Authentication prior to access to the Company's information systems.

"Unit Responsible for Internal Audit" Duties and Responsibilities

- Audit users' operations for compliance with the Company's information security policy, carried out under the standards and guidelines set out in the policy, and cooperate with the unit responsible for information system security and the policy in order to protect assets and data.
- Assist the unit responsible for information system security and the policy in identifying risks, including threats that may endanger security.

"Unit Responsible for Risk Management"

Has the duty and responsibility to analyze and assess the risks of information systems in order to improve the Company's quality and efficiency and to reduce the likelihood of potential damage.

"Unit Responsible for Legal Affairs"

Has a duty and responsibility to provide opinions or advice on regulations, requirements, rules, bylaws, laws, Acts, Royal Decrees, litigation, and infringements of intellectual property relating to information security.

"Unit Responsible for Human Resource Administration" Duties and Responsibilities

- Screen applicants' qualifications with respect to information system security violations.
- Have "personnel" sign agreements not to disclose the Company's confidential information.
- Report information on hiring, changes in employment status, resignation, death, transfer, and suspension or disciplinary action to the unit responsible for information system security, for the management of information system resources and access rights to applications.

"Unit Responsible for People Development and Corporate Culture"

Has the duty and responsibility to provide opinions or advice on regulations, requirements, rules, bylaws, laws, Acts, Royal Decrees, litigation, and infringements of intellectual property relating to the Company's information security.

"Unit Responsible for Buildings and Facilities"

Has the duty and responsibility to establish physical and environmental security, control entry to and exit from buildings and offices, and prepare protection against various threats, both human and natural, such as fire, flood, earthquake, civil unrest, etc.

Exception Management

Where a requirement cannot be complied with, an exception request shall be submitted, together with the reason, the risk, compensating controls, the duration, and the approver.

Exceptions shall be valid for no more than 12 months and shall be reviewed before every expiry.

Information Security Policy

5. Organization Controls (Annex 5)

Objective

This Information Security Policy and its related guidelines have been prepared to set the direction, principles and framework of requirements for protecting information-related assets against threats that may cause damage to the Confidentiality, Integrity and Availability of data and information systems; to drive robust internal controls over information in line with a Risk Based Approach consistent with international standards; and to encourage users to be aware of the importance of information security, including the importance of information risk management.

5.1 Policies for Information Security

A written information security policy shall be prepared to establish confidence and security in the use of information technology systems. The information security policy shall be approved by the Company's management, and the information security policy document shall be disseminated in writing to employees and relevant external parties for their acknowledgement and signature.

Review of the Policies for Information Security: The security policy shall be reviewed at the defined interval of at least once a year, and where significant changes occur, the policy shall be updated within 6 months, to ensure that the Company's employees are aware of the security measures relevant to their work.

5.2 Information Security Roles and Responsibilities

So that the Company defines the scope of its management, controls operations and carries out information security activities within the Company, including the security of remote working and the use of mobile computing devices, in order to manage the security of the Company's information and information processing facilities that are accessed, processed or used in communication with customers or external parties.

5.2.1 The duties and responsibilities of personnel in carrying out information security and technology service activities shall be clearly defined.

5.2.2 Management shall appoint a committee or core working group, together with the necessary resources, to manage and administer information security.

5.3 Segregation of Duties

Duties and areas of responsibility that could give rise to conflicts in operations, by enabling changes to the Company's assets or misuse of assets, whether without authorization or unintentionally, shall be segregated from one another to reduce the likelihood of such risk events occurring.

5.3.1 All employees and contractors shall be required to maintain information security and technology services by acting in accordance with the Company's established policies and guidelines, including:

5.3.2 Personnel shall be directed and supported to achieve the effectiveness of the information security and technology service management system.

5.3.3 The direction of policy implementation shall be set to establish security for information processes, and the information security and technology service management system shall be reviewed.

5.3.4 The resources necessary for the information security and technology service management system shall be provided for its operation.

5.3.5 The importance of an effective information security and technology service system, and of conforming to the defined requirements of the information security and technology service system, shall be communicated.

5.4 Contact with Authorities

A list of names and contact information for relevant people within the Company shall be defined for use when an emergency or disruption occurs that prevents the Company from operating normally.

5.5 Contact with Special Interest Groups

Contact with special interest groups, groups with expertise in information security, and professional associations shall be maintained so that contact can be made on an ongoing basis.

5.5.1 A list of names and contact information for special interest groups and groups with an interest in information security and technology services shall be defined, and the contact information shall be updated regularly.

5.5.2 A list of names and contact information for other agencies, such as the Royal Thai Police, Internet service providers, the Thailand Computer Emergency Response Team (Thai CERT), etc., shall be defined for use in security liaison and coordination when an incident occurs or when contact is necessary, and the contact information shall be updated regularly.

5.6 Threat Intelligence

5.6.1 The Company manages information relating to security threats, which is collected and analyzed to produce threat intelligence. This control requires the responsible persons to collect information about threats and analyze it to take appropriate mitigating actions. This information may relate to specific attacks, the methods and technologies used by attackers, and attack trends. The people responsible collect this information internally as well as from external sources.

5.6.2 The Company has defined a process for collecting threat information in order to assess risks and mitigate the risk of future events, and the Company reviews the collected information relating to information security and technology service threats every 3 months in order to keep pace with the constantly changing threat landscape.

5.7 Information Security in Project Management

In project management, regardless of the type of project, rules, regulations and requirements governing operations and access to data shall be defined so that project work is secure, such as defining users' access rights to data. Projects contracted to external companies, projects carried out by external parties, and in-house projects shall comply with the work procedure for information technology projects, so that project management is secure and the impact of potential risks is reduced, e.g. hiring Outsource services to develop programs.

5.8 Inventory of Information and Other Associated Assets

The inventory of information and other associated assets is an important document in the management of the Company's information security. The objective of this policy is to ensure that the Company's assets and information are recorded and stored correctly and securely.

5.8.1 Inventory of Assets

- An inventory of the assets under one's responsibility shall be prepared, and the inventory shall be reviewed, maintained and updated regularly, at least once a year, or when significant changes occur.
- The asset inventory shall cover 6 categories of information assets, namely:

    1) Hardware

2) Software
3) Data and Information
4) Network
5) Personnel
6) Facility

5.8.2 Acceptable Use of Information and Other Associated Assets

- Procedures for handling and storing information assets shall be defined to prevent data and information from being leaked or misused.
- Users should not discard or leave important information assets, such as documents and storage media, in insecure places, public places, or places where they can easily be seen, etc.

5.8.3 Handling of Assets

- Confidential data shall not be disclosed to others except where necessary for the performance of work.
- Employees should be mindful of protecting data stored on users' computers, particularly computers shared by more than one person. Such confidential data shall be protected by encryption or by any other appropriate means provided by the operating system or information technology system.
- Employees should keep confidential documents and storage media containing confidential data in lockable cabinets when not in use, especially outside working hours or when such documents or media must be left unattended at the desk.
- Confidential data shall be removed from processing devices, such as printers, photocopiers, etc., immediately.
- Employees shall not disclose confidential data to third parties except where the disclosure is covered by a non-disclosure agreement.
- Storage media and portable computing devices, such as USB drives, containing confidential data shall be looked after, protected and used with care.

5.8.4 Return of Assets

Company employees whose employment ends shall return all assets relating to computer systems, staff identification cards, entry/exit passes, keys, computers, peripherals, manuals and all related documents to their supervisor before the last day of employment.

5.8.5 Classification Information Control

Classification of Information: data under one's responsibility, in both Hardcopy and Softcopy form, shall be categorized by Sensitivity, Criticality and Legal Requirement, to protect information with appropriate methods.

The types of data, levels of criticality, data classification tiers, as well as access levels and access channels, shall be defined in writing and communicated to the relevant people. The Company defines the classification levels as follows:

Classification	Description
General Data (External Data)	Data that can be published or disclosed to the public without restriction and has no impact on the security, operations or reputation of the Company, such as Company history and vision, public relations information, etc.
Internal Data (Internal Use)	Data whose access and use is restricted to within the Company only and which cannot be disclosed or disseminated to third parties unless formally approved by an authorized person, such as policies and operating procedures, or meeting agendas, etc.
Confidential Data (Confidential)	Data that has been assessed as disclosable only to personnel within the Company have the relevant responsibilities, and to directly concerned third parties who have been granted rights. If disclosed

Classification	Description
	in whole or in part, it would cause damage to the Company, such as accounting and financial data, customer data and business management data, project data, procurement data and NDAs.
Sensitive Personal Confidential Data (Sensitive Personal Confidential)	Data that can identify an individual and is sensitive to privacy if disclosed, which may affect the data subject in terms of safety, privacy or legal matters, such as personal data, health data, and employee income data. It shall be handled in accordance with personal data protection laws and regulations (e.g. PDPA, GDPR), including stringent security controls in accordance with ISO/IEC27001.
Highly Confidential Data (Highly Confidential)	Data of the highest importance to the Company's business operations or advancement, which requires stringent protection and access restricted

	only to people authorized at the highest level, such as "operating results, long-term strategic plans, merger and acquisition data", including various contracts.

5.8.6 Labeling of Information Control

- Methods shall be established for producing and managing labels for labeling documents, data and information asset equipment related to information and communication technology management.
- Data in document form shall be appropriately controlled and secured from the start of printing, labeling, storage, copying and distribution through to destruction, and this shall be established as a procedure that personnel are required to follow, to ensure that the data is controlled and secured.

5.8.7 Information Transfer

5.8.7.1 Information Transfer Policies and Procedures

1. Define policies, operating procedures and supporting measures covering all types of communication channels.
2. Agreements on information transfer
3. Require people accessing the system to request a password from the system administrator to use the system, which password may be used only within a defined period.
4. Define the agreements, guidelines, procedures and duration of information transfer.
5. Record the date and time of information transfer between companies.
6. Restrict access to information once the transfer has been completed.

5.8.7.2 Electronic Messaging

Define methods to protect access to electronic data, including the transmission of electronic data over the network. Confidentiality or non-disclosure agreements:

1. Agreements or confidentiality contracts, or Non-Disclosure Agreements (NDA), shall be established in line with the Company's data protection requirements and shall be reviewed regularly.
2. Employees, individuals or contacts from other organizations who need to access the Company's information, shall be required to sign an agreement between "personnel" and "contacts" not to disclose the organization's confidential information (Non-Disclosure Agreement: NDA).

5.9 Access Control

To establish measures to control unauthorized persons from accessing the Company's information and communication technology systems; to prevent intrusion through the network by intruders and by malicious programs or code that may damage data or disrupt the operation of the information and communication technology systems; and to enable accurate auditing, tracking and identification of persons who use the Company's information and communication technology systems.

To ensure that access to information and information processing facilities is restricted, so that user access is controlled and limited to authorized persons only, and unauthorized access to systems and services is prevented, access rights to levels of data or information are defined in order to prevent access to all confidential data.

Policy

5.9.1 Controls over the use of data and information systems shall be established to control access so that only authorized persons may gain access.

5.9.2 Access rights to data and information systems shall be defined appropriately to the user's access needs and duties and responsibilities before the user accesses the information and communication technology systems, and access rights shall be reviewed regularly in accordance with procedures. Users shall obtain authorization from their supervisor based on their need for use.

5.9.3 Only system administrators may modify or change access rights to data and information systems.

5.9.4 Use of the Company's information and communication technology systems should be recorded and monitored, and security breaches affecting critical data and information systems should be monitored.

5.9.5 Details of system access and changes to rights, by both authorized and unauthorized persons, shall be recorded as evidence for investigation should a problem arise.

5.9.6 Rules, prohibitions and penalties regarding access to data and information systems shall be defined for those who violate the rules.

5.9.7 Access to the Company's data and information systems may be granted only upon approval by the person's supervisor, and the person may access only the data and systems relevant to their job duties. Data security and data confidentiality processes are considered part of the definition of information system policies and work procedures. These processes include the granting of rights and the management of access credentials, defining the scope of access to data or computer systems and other types of data storage devices, and the backup and recovery of damaged data.

5.10 User Access Management

5.10.1 User Registration and De-Registration

The registration of new users shall be governed by a formal procedure for registering new users so that they are granted the various usage rights as necessary, as well as a procedure for revoking usage rights,

for example upon resignation or upon an internal change of position. Such procedures shall be followed, and users shall be reviewed and approved strictly in accordance with the defined steps.

5.10.2 User Access Provisioning

For the management of user access rights, a method for managing access rights shall be defined; both the granting and the revocation of rights shall have a defined procedure for all types of users.

5.10.3 Management of Privileged Access Right

5.10.3.1 User rights to access each information system shall be defined, including rights segregated according to assigned responsibilities.

5.10.3.2 Users shall be authenticated every time they log on to an information system.

5.10.4 Management of Secret Authentication Information of User

5.10.4.1 There shall be a management process that protects the information delivered to users for authenticating themselves, which is confidential, as well as the safekeeping of their own secret information, and the delivery of user authentication information, which is Confidential information.

5.10.4.2 Employees of the Company shall comply with the procedure on registration for the use of information systems.

5.10.5 Review of User Access Rights

Access rights to information systems shall be reviewed at least once a year.

5.10.6 Removal or Adjustment of Access Rights

5.10.6.1 The access rights of employees and of personnel of external parties to information and information processing facilities shall be removed upon termination of employment, expiry of contract, or termination of the engagement agreement, and shall be regularly updated to remain accurate.

5.10.6.2 Access rights to information systems shall be reviewed at the intervals defined in the procedure.

5.11 System and Application Access Control

5.11.1 Information Access Restriction

5.11.1.1 The use of information within information systems shall be controlled, namely by defining usage rights such as write, read, delete, etc.; defining the groups of users who are permitted to use it; and verifying that the information permitted for use contains only the data necessary for use.

5.11.1.2 User accounts with special-level access rights to information systems, such as Root or Administrator, shall be assigned to users only after consideration of necessity, and only with an access period defined appropriately for the work.

Third parties shall indicate their consent to strictly comply with the Company's Information and Communication Technology Security Policy (ICT Security Policy) before being permitted to access information technology systems.

5.11.1.3 Secure log-on Procedure: systems shall be configured to delay service for 5 minutes if a user enters an incorrect password more than 3 times, and such events shall be analyzed and reviewed at least once a month to determine whether they constitute an attack.

5.11.1.4 Password Management System: a system or method shall be provided to check password quality, and there shall be a method to control and ensure that system users change their passwords at the defined intervals.

5.11.1.5 The use of Multifactor Authentications (MFA) for identity verification shall be required.

5.11.1.6 Where the information systems in use can use passkey devices (Passkey), their use shall be enforced in place of traditional passwords.

5.11.2 Use of Privileged Utility Programs

Rules and a control process shall be defined for the use of "Privileged Utility Programs" to prevent unauthorized access to or modification of systems and data, reduce the risk of privilege escalation and unapproved changes, and support the audit trail.

- The use of system utility programs should be controlled to prevent access by unauthorized people, as follows:
- Authentication shall be performed before use.
- Utility programs shall be segregated from application programs.
- The use of utility programs shall be restricted to assigned people only.
- Details of access to utility programs shall be recorded, such as the system user, etc.

5.11.3 Access Control to Program Source Code

Information system developers should provide access control over the Source Code of systems in production or in service, for example:

- Source Code should not be stored on production machines, and Source Code should be stored in a secure location.
- Source Code that is under testing shall not be stored together with Source Code that is already in production.

5.11.4 Access to Network and Network Services

Users

- Users shall be granted access only to the networks and network services for which they have been approved.
- Users who wish to connect a computer or device to the computer network system of the organization shall obtain permission from the head of their unit and shall comply with this policy, and users shall complete the "Network Connection Request" form.
- Requests to use Web Server space or a Sub Domain Name for which the unit is responsible shall be made by a written request for permission from the head of the unit, and no program shall be installed that affects the operation of the system or other users.
- No person shall move, add installations to, or take any action on central equipment, namely routing devices (Router), data switching devices (Switch), and devices connected to the core network system, without permission from the system administrator.

System Administrators

System administrators shall control access to the network system to manage the network system effectively, as follows:

- Usage rights shall be restricted to control users so that they can use only the network systems for which they are authorized.
- Access paths to shared network systems shall be restricted.
- The use of network paths from computers to server computers shall be restricted so that users cannot use other paths.
- All network systems of the organization that connect to other network systems outside the organization shall connect through intrusion prevention devices, which shall also be capable of detecting malicious programs (Malware).
- The network system should have an intrusion detection system (Intrusion Prevention System / Intrusion Detection System) installed to monitor abnormal usage by people accessing the organization's network system.
- Access to the organization's internal network system via the Internet shall require logging in (Login) by identifying oneself with a username, and authentication (Authentication) by password shall be performed to verify the user's validity every time beforehand.

- External organizations that are connected shall be prevented from seeing the internal IP Addresses of the organization's internal network system.
- A network diagram (Network Diagram) shall be prepared, containing details of the boundaries of the internal network and external network and of the various devices, and shall always be kept up to date.
- Identification of devices on the network:
- System administrators maintain a register of network connection requests, namely the list of requesters, details of the computers requesting service, IP Address, and installation location.
- Devices that are connected will be assigned an IP Address as specified by the network administrator.
- System administrators shall restrict the users who can access devices.
- In the case of devices connecting from an external network, the device number shall be identified as to whether it is permitted or not permitted to connect to the internal network.
- Network devices shall be able to verify the IP Addresses of both the source and the destination.
- Requesters shall complete the "Network Connection Request" form via Inception or contact the Company's IT Department.
- Access to devices on the network shall require authentication every time the device is used.

A time limit shall be set for users on the network system, whereby they are logged out of the network system when:

- Idle for no more than 15 minutes.

System administrators shall manage and control server computers (Server) and shall be responsible for maintaining server computer systems (Server) regarding defining, modifying, or changing the various settings of systems software (Systems Software).

The installation or update of application software shall require approval from the system administrator before installation is carried out.

Source code, ready-made code packages, and documentation for application software shall be stored in a secure location.

Computer traffic data (Log) shall be retained so that computer traffic data is accurate and can identify individuals, in accordance with the computer-Related Crime Act B.E. 2550 (2007) and amendments.

Measures shall be defined to control the use of the network system and server computers (Server) by users from outside the organization, to maintain system security, in accordance with the following guidelines:

- People from external organizations who require rights to access the organization's network system and server computers (Server) shall submit a written request for permission to the head of the unit.
- Ports (Port) used to access the system shall be strictly controlled.
- Any method that allows remote access to data or data systems shall be authorized by the head of the unit.
- For remote access, users shall present evidence and adequately state the reasons or necessity for their work with the organization.
- Remote access to the internal network system and the organization's information systems shall require logging in (Login) by identifying oneself with a username, and authentication (Authentication) by password shall be performed to verify the user's validity every time beforehand.
- Access to networks and network services shall be specifically controlled to maintain the security of data and information technology systems, for example the use of secure protocols for network management such as Secure Socket Layer (SSL), Simple Network Management Protocol (SNMP), and Web Certificate.
- Network use that affects Bandwidth shall be restricted, such as sending and receiving large files, listening to music online, watching TV online, or playing online games during normal working hours.
- The network system should be appropriately designed and configured to maintain the security of information and information technology systems; for example, all devices connected to the network system should be securely configured, and activities related to the network system shall be monitored. Cabling systems shall meet industry standards and be installed by approved skilled personnel. Network devices such as:
- Router, Firewall, Switch, and Wireless Access Point shall be configured according to the security requirements of each device or according to the manufacturer's recommendations, or those of bodies such as the SANS Institute or the National Security Agency (NSA: National Security Agency).

Protection of the network and of the devices connected to the network system shall be clearly defined, and the configuration of various parameters, such as IP Address, shall be reviewed at least once a year. In addition, all relevant people shall be notified every time parameter values are defined, modified, or changed.

All network systems connected to other network systems outside the organization shall connect through intrusion prevention devices or Packet filtering programs, such as a Firewall or other hardware, and shall also be capable of detecting malware (Malware).

An intrusion detection system (IPS/IDS) shall be installed to monitor abnormal usage by people accessing the organization's network system, including monitoring of intrusions via the network, abnormal usage, and modifications or changes to the network system by people without relevant authority.

The IP addresses of internal network systems should be protected so that connected external organizations cannot see them, to prevent outsiders from easily learning about the structure of the network system.

The use of tools (Tools) for examining the network system shall be approved by the system administrator and restricted to use only as necessary.

5.11.5 Identity Management

To enable the unique identification of each individual and of the systems that access the Company's information and other associated assets, and to enable access rights to be assigned appropriately:

The Company should have supporting processes to manage changes to information related to user identities. These processes may include verification of trusted documents relating to the individual.

When using identities provided or issued by third parties (e.g. credentials on social media, etc.), the Company should ensure that third-party identity information provides an appropriate level of trust and that any associated risks are known and adequately treated. This may include controls related to third parties as well as controls related to authentication information.

5.11.6 Authentication Information

5.11.6.1 Management of Secret Authentication Information of User

5.11.6.2 Those who manage user accounts shall keep users' passwords confidential. Those who manage user accounts shall define the password format to be at least 8 characters long or more, combining lowercase letters, uppercase letters, digits, and special characters such as ! @ # $ % ^ & * to make them difficult to guess. Words found in the English dictionary (Dictionary) shall not be used; personally identifiable information such as telephone numbers, dates of birth, or national ID card numbers shall not be used; and consecutive sequences of letters or digits, such as abcd, 1234, abcd1234, etc., shall not be used.

5.11.6.3 When assigning a password to a user for the first time, the person who manages user accounts shall assign a randomly generated temporary password.

5.11.6.4 The password shall be communicated directly to the user on their first day of work, or when a password reset is requested through the password management system.

5.11.6.5 Users shall be instructed to change their password immediately upon first use.

5.11.6.6 Systems that support MFA shall have it enabled, particularly Email, VPN, Admin console, and critical data systems.

5.11.6.7 Account lockout / limiting password guessing: after more than 5 failed attempts, the account shall be temporarily locked for 5–15 minutes depending on the cycle of failures.

5.11.7 Use of Secret Authentication Information

The use and safekeeping of user authentication information shall be carried out in accordance with the Company's policy or procedures for the use of secret authentication information, for example:

- Username and Password information shall be kept confidential and shall not be disclosed to any other person.
- Avoid keeping a record of such information unless it can be stored securely.
- When receiving Username and Password information that is Default information, it should be changed immediately upon first access to the system.

5.12 Information Security in Supplier Relationships

5.12.1 Information Security Policy for Supplier Relationships

The use of services from external service providers may give rise to risks, such as the risk of access to data, the risk of data being modified incorrectly, and unauthorized processing by application systems. It is therefore necessary to control external service providers who access the Company's information and communication technology systems so that such access is secure, and to define guidelines for the selection and control of the work of external service providers.

Information security requirements for mitigating the risks associated with supplier access to the Company's assets shall be agreed with the service provider and documented in writing.

- The Company shall define an information security policy relating to external service providers, whereby the relevant persons shall consider or assess the risks that may arise and define preventive measures to reduce those risks before permitting external service providers or third parties to access the information systems or use the information of the Company.
- System administrators and the various departments responsible for coordinating with external service providers shall oversee and ensure that people or external service providers engaged by the organization comply with the specified contract or service agreement, which shall cover security work, the nature of the service, and service levels.

5.12.2 Control of Access by External Service Providers (Third Party)

5.12.2.1 The Information and Communication Technology Department shall assess the risks arising from access to information technology systems or processing equipment and shall have appropriate support or corrective measures in place before permitting access to the systems.

5.12.2.2 External service providers (Third Party) requiring rights to access the Company's data sources shall submit a written request for approval from the department manager and the office of the data owner, who are responsible for all actions of such people. The request shall contain at least the following details:

- Reason for the request
- Period of use
- Security check of network connection devices
- Defined protection against disclosure of information

5.12.2.3 External service providers (Third Party), whether working inside or outside the Company, shall sign an agreement to protect the Company's confidential information.

5.12.2.4 System owners are responsible for defining and reviewing access rights to information systems for necessary people only, and for reviewing rights to keep them up to date.

5.12.2.5 The Company shall consider conducting risk assessments of, or establishing internal controls over, external service providers, depending on the importance of the information technology system.

5.12.2.6 The Company has the right to audit in accordance with the service contract to ensure that the Company can comprehensively control usage in accordance with that contract.

5.12.2.7 In the event of a change in operations, the external service provider shall notify the Company and obtain the Company's approval of the change before carrying it out, to ensure that it remains within the defined scope.

5.12.2.8 Upon the end of the period of use, the Company shall revoke the rights to access data sources and notify the department manager and the data owner.

5.12.2.9 If an information security breach is found, it shall be reported to the system owner.

5.12.2.10 The information security policy announced by the Company shall be strictly complied with.

5.12.3 Assessing Security within Supplier Agreements

Information security requirements shall be defined and agreed with external service providers in matters relating to access, processing, storage, communication, and the provision of system infrastructure services for the Company's information by external service providers.

- The Company shall present its information security policy to external service providers in relation to access, processing, storage, communication, and the provision of the Company's information services.
- External service providers shall accept the Company's policies, relevant laws, and security controls.
- The Company has the right to inspect the working environment, including auditing the work of external service providers.

5.12.4 Information and Communication Technology Supply Chain

- Agreements with external service providers shall include requirements for identifying risks arising from the information and communication technology service supply chain.
- Risks arising from access to data and information systems or processing equipment by external parties shall be assessed, and appropriate control measures shall be defined before permitting access to such data and information systems or equipment.

5.12.5 Supplier service delivery management

To maintain the agreed level of security and service delivery in accordance with the service agreements of external service providers.

Monitoring and review of Supplier Services

- The Company shall establish an agreement defining the Company's right to inspect the working environment, including auditing the work of external parties, based on the procurement contracts of the external parties.
- The delivery service of external service providers should be regularly reviewed, monitored, and audited.

Managing Changes to Supplier Services

- Every change to the service details of external parties relating to the Company's information services shall be in accordance with the documentation.
- Changes to the services of external service providers, including updates to current policies, procedures, and measures, shall be managed, considering the criticality of the information and the business processes involved, and the risk assessment shall be reviewed again.

5.12.6 Information Security for using Cloud Services

The Company controls security requirements for cloud services to better protect the Company's data in the cloud, including the acquisition, use, management, and termination of cloud services. The Company establishes security measures for cloud services and defines criteria for selecting cloud service providers. In addition, the Company defines a process for considering acceptable cloud usage and defines information security and technology services upon termination of cloud services, with the following requirements:

- The Company permits the use only of cloud services that have passed a risk assessment and been approved under the Cloud Service Onboarding process, and that are on the Approved Cloud Services list.
- Cloud services that store/process data classified as Confidential or higher shall enforce MFA, logging, and encryption at rest/in transit, and access rights shall be reviewed at least quarterly.
- Before terminating a cloud service, an Exit Plan shall be prepared to migrate/return data, revoke access rights, and securely delete data, with evidence of the actions taken recorded.

5.13 Management of Information Security Incidents and Improvements

To ensure that events and weaknesses related to the security of the Company's information systems are handled correctly within an appropriate time frame, and that there is a consistent and effective approach to the management of the Company's security incidents:

- The Company shall define responsibilities and establish procedures to respond to security breaches in a timely manner.
- The Company shall require that undesirable or unexpected information security situations be distinguished from general operational events to define correct and appropriate corrective approaches.
- The Company shall define channels and criteria for reporting events, weaknesses, or information security events, or for communicating them to personnel within the organization and to external parties.

5.13.1 Other Acts Prohibited by the Company

- Any act defined by law as an offence, as well as other acts of the kinds mentioned below, are prohibited by the Company, and employees are not permitted to carry them out. The Company has not listed all prohibited acts; this list is intended only as a guideline for users.

Note: Some employees may be exempted from certain of the prohibitions mentioned below (insofar as this does not conflict with the law) if they are acting in the performance of assigned

duties; for example, system administrators may suspend the network access of any device if such access disrupts the operation of information technology systems.

- Using the Company's resources to obtain or forward pornographic or obscene materials, documents, or images, or those that are contrary to law.
- Fraud using the User ID and password assigned by the Company to offer any goods or services for sale.
- Attempting to breach security or disrupt the operation of the network system. Examples of security breaches include accessing data or server computers that one is not authorized to access, etc. Examples of disrupting the operation of the network system include Sniffing, Pinged Floods, Pack Spoofing, Denial of Service, and Forged Routing Information with malicious intent, etc.
- Using large amounts of Bandwidth, especially using P2P File Sharing programs.
- Performing Port Scanning and Security Scanning, except when carried out in the performance of assigned duties.
- Eavesdropping on or intercepting data that the employee is not authorized to know by any means, except when carried out in the performance of assigned duties.
- Searching for system flaws in order to gain unauthorized access to data or systems.
- Circumventing user authentication or the security measures of any computer or network system.
- Using any program/script/command or sending any message with the intent to disrupt, degrade service performance, or suspend the use of users, whether through internal systems or through various network systems.
- Providing confidential information concerning employee lists, customer lists, Company secrets, and other confidential information to third parties.
- Threats and harassment of any kind via e-mail, telephone, or messaging systems, regardless of the language, frequency, or size of the messages; posting comments or sending any messages unrelated to work to many people (Newsgroup Spam).
- Infringing personal rights, the Company's copyrights, the Company's trade secrets, patents, intellectual property, or any other law.

5.13.2 Reporting information security weaknesses

Employees and contractors who use the Company's information systems and services shall observe and report any observed or suspected information security weaknesses in systems or services. Events are classified into levels as follows:

- Low-level event criteria

The department's information system administrator can resolve the event themselves, e.g. a virus infection, etc., and shall report the events that occurred every 1 month.

- Medium-level event criteria

The department's information system administrator shall notify their supervisor of the event that occurred. Once the department has assessed the risk of the event, the department shall notify the Company's IT Department in writing so that it can intervene to resolve the event.

- High-level event criteria

The department's information system administrator shall urgently notify the Company's IT Department if the event is serious and urgent, to find a solution to the problem, and shall then summarize the problem that occurred with the department's information systems for senior management.

5.13.3 Assessment of and decision on information security events

Information security situations shall be assessed, and a decision shall be made as to whether the situation constitutes an information security event, through the following process:
IT Department Manager: shall establish policies for personnel and system administrators in the respective units to comply with the established policies.

- System administrators shall provide for the monitoring and maintenance of intrusion detection and prevention devices; abnormal events and alerts detected by the devices will be analyzed and the causes of intrusion into the Company's information systems determined, to serve as an investigative tool to identify persons who attack, intrude, or misuse the system.

System administrators: shall provide for the monitoring and maintenance of intrusion detection and prevention devices, abnormal events, and the alerts detected by the devices.

- System administrators shall keep statistics on attempts to intrude upon or attack the system, as a tool for measuring the protective effectiveness of other security systems, such as firewalls, etc., and to protect the internal computer network from dangers originating from external computer networks, such as intruders or hackers, as well as various types of viruses.

System administrators: System administrators shall manage system intrusions by prioritizing intrusions according to their impact on the Company.

- System administrators shall manage system intrusions by prioritizing intrusions according to their impact on the Company and shall establish correct procedures for the Company to prevent recurrence of such events.

5.13.4 Response to information security incidents

Information security incidents shall be responded to deal with the problem in accordance with documented procedures.

- Procedures are defined to handle cases where an event has been assessed as causing insecurity.
- When an information security incident occurs, it shall be responded to dealing with the problem in accordance with documented procedures, which have been prepared separately for each system as follows:
- Intrusion prevention system: examine the Log Files or reports of the intrusion prevention system. The items to be examined are as follows:
    - How many attacks there are, and which type of attack is most frequent
    - Whether the attacks that occurred follow a predictable pattern
    - The level of severity
    - The network IP addresses used by malicious actors to attack
- Firewall system: examine the intrusion prevention system at least once a month and examine the Log File records and firewall reports. The items to be examined are as follows:
    - Packets that the firewall has Blocked
    - The characteristics of the Blocked Packets
    - Packets from which network IP addresses have been Blocked in large numbers

Note: If an attack on the system or an information system security breach is detected, the head of the unit shall be notified to decide on corrective action.

- Internet threat or malware (Malware) protection system, comprising viruses, internet worms, Trojans, and spyware: examine the Log Files and reports of devices related to the internet threat protection system. The items to be examined are as follows:
    - Which types of malwares are found in large numbers
    - From which network malware was sent, and to where it was sent
    - Whether malware is being sent from the Company's internal network to the outside

- Study methods to remediate computers infected with malware, especially types detected as spreading within the Company's network
- If a computer within the network is found to be infected with malware or to be sending malware outside, the infected machine shall be disconnected from the network system and remediated immediately

5.13.5 Learning from information security incidents

Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future security incidents.

- System administrators shall record security breaches, weaknesses, vulnerabilities, threats, or malfunctions of information systems, as well as the methods used to resolve the events that occurred, to prepare necessary preventive measures in advance.
- The unit responsible shall prepare a summary report of security breach notifications for supervisors at least once a month.
- Security breaches shall be reviewed to prevent recurrence of the same problems.
- Risk analysis and assessment of intrusion/breach/outbreak situations related to information system security shall be carried out at least once a year.

5.14 Collection of Evidence

The Company shall define and apply procedures for the identification, collection, acquisition, and preservation of information that can serve as evidence.

The unit responsible for information system security and for the policy shall ensure that units with critical information systems collect and preserve evidence in accordance with the rules or criteria for retaining evidence for reference in analysis and

investigation, or as evidence in relevant court proceedings, when an event is found to be related to civil or criminal legal action.

Units with critical information systems shall retain data to serve as reference evidence that they have complied with the defined rules, regulations, or requirements, with retention periods according to the importance of the data, the Company's regulations, and the law (e.g. 90 days, etc.).

The head of the unit responsible for legal matters and units with critical information systems shall study the relevant rules, such as statements in civil or criminal law that specify the nature of the evidence to be collected for use in legal proceedings against offenders, etc.

Units with critical information systems shall study the characteristics of evidence that is complete and of good quality so that it can be used in court proceedings.

5.15 Information security during disruption

5.15.1 Information Security Aspects of Business Continuity Management

To serve as guidelines for managing the continuity of the Company's operations under crisis conditions and various emergencies, ensuring that the Company's critical operating procedures and information systems have an appropriate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), so that the Company's operations can continue without interruption.

5.15.2 Information security continuity

Planning information security continuity

- The Company shall determine its requirements for information security and for continuity in adverse situations, such as during a crisis or disaster.
- Guidelines shall be prepared for developing emergency response plans for information technology systems, which should consider the following:

Preparedness to prevent and reduce the likelihood of events that cause damage and affect the Company's operations and the Company's information technology services.
Response to emergency situations to control and limit the extent of damage, e.g. defining guidelines for controlling and resolving emergency situations, etc.
Actions to enable the Company to continue operating, e.g. backup of data and critical equipment, recovery of damaged application systems and data, etc.
Return to normal operations to bring the Company's operations back to normal conditions, e.g. defining guidelines for restoring damage to return to normal operations, etc.

5.15.3 Implementing information security continuity

The Company shall establish, document in writing, implement and maintain processes, procedures and controls to achieve the defined level of security continuity when a disruptive situation occurs.

- An ISS (business continuity plan management team) for information technology systems shall be established, consisting of representatives from departments, data owners, system owners, data custodian units, etc.
- The ISS (business continuity plan management team) shall prepare a written contingency plan for information technology system emergencies, keep it always updated, and arrange for the plan to be tested at least once a year.
- Verify, review and evaluate information security continuity

The Company shall verify the continuity controls that have been prepared at defined intervals to ensure that those controls remain valid and effective when a disruptive situation occurs.

- Backup media, together with copies of the various procedures or work instructions, shall be stored off-site.
- Where data must be retained for a long period, consideration shall also be given to the method of retrieving the data for use in the future.
- Labels with clear details should be affixed to backup media so that they can be located quickly and to prevent erroneous use of the media.
- Requests to use backup media should be approved by an authorized person, and a register should be maintained to control the receipt and handover of backup media.
- Procedures shall be defined for the destruction of important data and of media that are no longer in use, including important data on hard disks.

5.16 Redundancies

5.16.1 Availability of information processing facilities

- Application systems/processes are prioritized, with the interrelationships of each system and the recovery time of each system determined through risk assessment and/or business impact assessment of core processes.
- Scenarios or problem severity levels are defined.
- Detailed problem-resolution procedures exist for each scenario.
- Responsible personnel and decision-making authorities are designated.
- Details of the equipment required in an emergency for each application system are documented.
- Units that serve as data backup or data storage units shall also clearly specify details of the backup computer centre.
- The contingency plan is regularly reviewed or updated to keep it current (every 6 months), and the contingency plan is kept in a secure location.
- Execution of the contingency plan is tested at least twice a year, and the tests shall take the form of real-situation simulations.
- The contingency plan shall be communicated to relevant people at all levels only on a need-to-know basis, and persons without relevant authority or duties should be prevented from gaining knowledge of it.
- When an emergency occurs, details of the event, the cause of the problem and the method of resolution should also be recorded.

5.16.2 ICT readiness for business continuity

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements, and requirements should be controlled so that the Company's information and communication technology is ready for potential disruptions, ensuring that necessary information and assets are available when needed. This includes readiness planning, implementation, maintenance and testing.

The Company has defined processes and planning procedures that consider risks and business requirements for recovery.

The Company has defined maintenance for information technology and testing procedures for disaster recovery and business continuity plans, and such plans have been approved by the Director and Assistant to the Chief Executive Officer.

The Company has prepared documentation through business impact analysis, business continuity strategy and business continuity plans, together with business continuity test reports, with business continuity reviewed and tested at least once a year.

5.17 Legal, statutory, regulatory and contractual requirements

To prevent breaches relating to operations, regulations, rules, contractual terms and requirements relating to information security, and to serve as guidelines for the Company's operations in line with the information security policy.

5.17.1 Compliance with Legal and Contractual Requirements

Identification of Applicable Legislation and Contractual Requirements

The Company shall study and define a list of policies, rules, regulations, laws or contracts relating to the use of information and communication technology by its departments.

All employees shall acknowledge, understand and strictly comply with the defined list of policies, rules, regulations, laws or contracts relating to the use of information and communication technology, which shall include at least the following:

- Electronic Transactions Act B.E. 2544 (2001) and amendments
- Computer-Related Crime Act B.E. 2550 (2007) and amendments
- Copyright Act B.E. 2537 (1994) and amendments
- Personal Data Protection Act B.E. 2562 (2019)
- Royal Decree Prescribing Security Procedures for Electronic Transactions B.E. 2553 (2010)
- The Company's information security policies and guidelines
- Regulation of cryptographic controls

- Cryptographic controls shall be applied in accordance with relevant agreements, laws and regulations.

Data created, stored or transmitted through the Company's information technology systems are considered assets of the Company (except data that are assets of customers or third parties, including software or other materials protected by third-party patents or copyrights). The Company may disclose or use such data as evidence in investigations of any offences without the need to notify users in advance.

For the purposes of managing and maintaining the security of the Company's information technology systems, the Company reserves the right to inspect users' use of computers, computer systems and network systems to ensure that usage is in accordance with the Company's policies.

The Company reserves the right to access, review and inspect users' email without the need for prior notification. However, the Company will carry out such inspection only when necessary and will not disclose any information of users except where disclosure is pursuant to a court order under mandatory provisions of law or with the user's consent.

Employees of the Company are prohibited from using the Company's assets and information technology systems to perform any act that contravenes the laws of the Kingdom of Thailand or international law under any circumstances.

The transfer of software, confidential information, encryption software or any technology out of the country must not contravene any laws of the Kingdom of Thailand, international law or the laws of the destination country. Users shall consult their supervisor and legal experts before carrying out any export.

5.18 Intellectual Property Rights

Intellectual property rights and the use of proprietary products shall comply with legal procedures, regulations and private contracts.

The Company shall comply with copyright requirements in the use of intellectual assets procured by its departments, and shall take care never to infringe such copyrights.

The Company shall strictly comply with the requirements specified in software licences (Software Copyright) and shall also control the use of software in accordance with the licences obtained, namely: registration for software use; retention of evidence of licence ownership; and regular checks to verify that installed software is properly licensed.

Users are strictly prohibited from reproducing or distributing any images, songs, articles, books or documents in a manner that infringes copyright, or installing pirated software on the Company's information technology systems.

To ensure that employees of the Company do not infringe copyright unintentionally or inadvertently, they should not copy any software installed on the Company's computers for any purpose whatsoever without authorization, and

at the same time employees of the Company should not install any program on the Company's computers without authorization, in order to ensure that licences covering such installation exist.

The Company requires computers to be inspected at least once a year to check the list of software on each computer and to ensure that the Company holds a licence for each software product on the computer. If unlicensed software is found, such software will be removed, and if necessary, the Company may consider replacing it with other properly licensed software.

5.18.1 Protection of Records

The Company shall retain records to serve as evidence of compliance with the defined rules or regulatory requirements, with retention periods according to the importance of the records, the Company's regulations on correspondence and records management, and the law.

5.18.2 Privacy and protection of personally identifiable information

The Company shall protect data and privacy in accordance with the laws, regulations and contracts relating to the Company.

5.18.3 Protection of Organizational Records

The Company's important records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized disclosure.

Users of the Company's important records shall act in accordance with the law and with the Company's policies, rules and regulations.

5.18.4 Regulation of cryptographic controls

The Company shall apply cryptographic controls in accordance with relevant agreements, laws and regulations.

5.18.5 Prevention of Misuse of Information Processing Facilities

The Company's information processing facilities are provided solely for the Company's business, except where a user has been granted specific permission by an authorized supervisor.

Responsible persons shall be designated, and an inventory of information processing facilities purchased or leased for use shall be prepared.

Documents or registers controlling equipment shall be updated whenever changes occur, to serve as information for controlling the Company's assets.

Any action involving the installation of additional software or equipment shall be approved in writing by an authorized supervisor to prevent unauthorized changes.

Information processing facilities shall, at a minimum, have a means of verification for authentication prior to access, by entering a password in accordance with the password management policy.

5.18.6 Independent Review of Information Security

The Company's approach to managing information security and technology services, and its implementation, shall be reviewed — for example, reviewing objectives, controls, policies and work procedures to ensure that they are correct and up to date — at defined intervals of at least once a year.

5.18.7 Compliance with policies, rules and Security Standards for information security

Compliance with Security Policy and Standards

- All systems of the organization shall be audited in accordance with the information security policy and at the defined intervals.
- Policy documents, controls, work procedures and related forms shall be inspected and reviewed at defined intervals or when changes occur.

5.18.8 Technical Compliance Review

The technical details of systems already in use or in service shall be inspected at defined intervals to determine whether information security and technology services are adequate, including checking whether systems can be intruded upon and whether the configuration of system parameters is secure, as well as inspecting systems using vulnerability scanning software (Vulnerability Scanning) and penetration testing (Penetration Test) to identify system weaknesses.

5.18.9 Document Operating Procedures

Appropriate guidelines shall be documented for each information technology system under one's responsibility and announced to the personnel performing the work.
Manuals and work guidelines shall be updated when procedures or the persons responsible for the work change, and all work guidelines and related documents shall be reviewed at least once a year. Information or documents relating to information technology systems shall also be protected from unauthorized access.

6. People Control Annex 6

Objective

To ensure that employees and contractors understand their duties and responsibilities and are suitable for the roles for which they are considered; that they are aware of and fulfil their information security responsibilities in order to reduce the risk of error and misuse by employees; and to ensure that the process of change or termination of employment does not affect information security.

6.1 Prior to Employment

6.1.1 Screening

Screening (background verification checks) of job applicants shall be carried out in accordance with relevant laws, regulations and ethics, and shall be proportional to business requirements, the classification of the information to be accessed and the associated risks.

The Company shall define information security duties and responsibilities in the qualifications of personnel according to their assigned job functions.

The Human Resources Management and Development Department shall verify the qualifications of all job applicants before they are appointed as personnel of the Company, which shall include criminal record checks or other checks according to relevant conditions.

The Human Resources Management and Development Department shall arrange for a Non-Disclosure Agreement (NDA) to be signed between the "employee" and the Company undertaking not to disclose the Company's confidential information. This signing shall form part of the employment of that employee and shall be binding both during employment and continuously after the end of employment in accordance with the personal data retention and retention period policy (SKY ICT Data Retention Policy).

6.1.2 Terms and Conditions of Employment

The terms and conditions of employment contracts with employees and contractors shall state the information security duties and responsibilities of the employee, the contractor and the Company. The Human Resources Management and Development Department shall define terms of employment that include the Company's information security duties and responsibilities.

The Human Resources Management and Development Department shall prepare information relating to the Company's information security policy for new employees and users to study and sign in acknowledgement, including accepting an agreement to strictly comply with the information security policy in the parts relevant to their position, duties and responsibilities under those policies.

To ensure that User ID management is correct and as up to date as possible, the Human Resources Management and Development Department shall immediately notify the responsible unit when any of the following occur:

- Hiring
- Change in employment status
- Resignation, or end of tenure as management, employee or staff, or death
- Transfer between departments
- Suspension, disciplinary action or suspension from duty

All new board members, directors, deputy directors, department managers, employees and staff who come to work at the Company shall sign to acknowledge and agree to comply with the Company's confidentiality agreement and other related documents before being permitted to start work or to access and use the Company's information.

6.2 During employment

Management responsibilities: Management shall require all employees and contractors to maintain information security by strictly complying with the policies and procedures established by the Company.

6.2.1 Information Security Awareness, Education and Training

All employees of the Company and relevant contractors shall receive information security awareness, education and training, and shall learn and receive additional refreshers on the Company's policies and procedures relevant to their work.

All employees of the Company shall receive training, with content appropriate to each individual's role and job functions, in order to build awareness and provide information security training.

Training shall be provided to employees on awareness and practices for securing information and communication technology systems, including notification of the security policy and changes in information and communication technology.

All new employees shall receive training on the information technology system security policy and the relevant departmental procedures before, or at the latest within 90 days of, starting work in the department. This should form part of orientation, and shall be signed for and kept in the personnel file.

The Human Resources Management and Development Department is responsible for informing personnel about the information technology system security policy and about changes relating to the security of information and communication technology systems.

6.2.2 Disciplinary process

A disciplinary process shall be formally established and communicated to employees, and employees shall agree to comply with the defined conditions, in order to take action against employees who violate the Company's information security.

The Company has measures in place to deal with persons who contravene or violate the Company's information security policy, which constitutes a disciplinary offence under the Company's rules and regulations, in the case of carrying out activities relating to testing information systems in order to check or enhance the security of information systems and networks, such as vulnerability scanning (Vulnerability Scan), penetration testing (Penetration Test), password cracking attempts, decryption attempts, network traffic inspection, etc. However, where such activities are performed with authorization or as part of the person's assigned duties for the Company, this is an exception.

6.3 Responsibilities after Termination or Change of Employment

6.3.1 Termination or change of employment responsibilities

Upon termination or change, all relevant parties shall be notified that the employee has changed role or left their position.

Access rights to information and information systems shall be revoked immediately upon the due date for retaining information and responsibilities.

- Accounts on the Portal system, the ERP system and fingerprint scanners of departing employees will be revoked at midnight on the last day on which the employee remains an employee of the Company.
- In the case of urgent revocation of rights, this will be carried out immediately upon notification.

Information security responsibilities that remain in force after termination or change of employment shall be defined and communicated to the employee or contractor, and compliance shall be enforced accordingly.

Employees shall return Company equipment in their care to the Company in complete condition. If, upon inspection, the equipment is found to be in incomplete condition, the employee shall be deemed responsible for the incomplete part, in accordance with the framework for disclaimer of liability for that part.

Employees whose employment has ended or whose duties have changed shall not wrongfully disclose the Company's confidential information after the end of their employment. If a breach of this requirement is found, the penalties prescribed by the Company shall be applied and pursued to the fullest extent.

6.3.2 Confidentiality or Non-Disclosure Agreements

Written confidentiality agreements or contracts, or Non-Disclosure Agreements (NDA), shall be established with employees within the Company and with external service providers to protect the security of information, and shall be appropriately reviewed and documented in writing.

6.3.3 Teleworking

Access control for work performed outside the Company: where an external service provider (Third Party) uses Remote Access to perform temporary work, the Information and Communication Technology Department shall comply with the Information Security in Third Party Relationship Policy by strictly controlling and monitoring use of, or access to, systems according to the rights granted.

Connections from outside the Company shall be approved and shall connect only through the Virtual Private Network (VPN) system permitted and provided by the Company. Users are strictly prohibited from changing the program used for connection.

The right to use Remote Access for temporary work is a right that the Company grants to users and external service providers on a temporary basis only and is not transferable.

Users of the Remote Access system shall obtain approval from their supervisor before using Remote Access. To access information systems, users shall specify a clear purpose, method of access and scope of access, and approval shall be granted per occasion or for a limited period, depending on the case and necessity.

The Company has the right to claim damages from users or external service providers if the Company's computer systems are damaged by a computer virus infection resulting from the use of Remote Access for temporary work.

6.3.4 Information Security Event Reporting

Information security events shall be reported through appropriate management channels as quickly as possible.

- Users shall report events relating to the Company's security through the defined reporting channels as quickly as possible, in accordance with the work procedure document on information security incident management.
- All users and third parties have a duty to report any security breach, weakness or inappropriate act that occurs or is suspected to have occurred within the Company to their supervisor or the Security Management unit immediately upon discovery, so that the problem can be addressed in a timely manner.
- Users who discover or become aware of abnormal operation, errors or weaknesses in software shall report them to the IT-Security officer immediately.
- Users who discover that any hardware or equipment is damaged or operating abnormally shall report it to the relevant unit immediately.
- Users and third parties who discover any security breach or weakness in the Company shall not disclose the event to others, except to their supervisor, the Security Management unit or the IT-Security officer, and are prohibited from attempting to prove suspected security weaknesses themselves.

7. Physical Controls Annex 7

7.1 Physical and Environmental Security

Objective

To ensure prevention of unauthorized physical access, damage and interference affecting the Company's information and information processing facilities; to prevent loss, damage, theft or compromise of assets; and to prevent interruption to the Company's operations.

To establish control and protection measures, and security standards relating to the use of or access to buildings, premises and information technology system areas, taking into account the importance of information technology equipment and of information, which is a valuable asset that may need to be kept confidential. These measures apply to users and external service providers.

7.2 Secure areas

General requirements

- Information system areas shall be classified and defined as specified, and a layout plan showing the location and type of information system areas shall be prepared for monitoring, control and protection against unauthorized persons, as well as to prevent other damage that may occur, and shall be announced to all concerned.
- Security equipment shall be installed, consisting of CCTV cameras, Access Control systems or equipment capable of preventing threats from intruders, etc., in the Company's information system areas, namely the Server/Data Center room, in order to comply with security standards. Departments shall determine the installation of information technology equipment in "information technology system areas" in line with the category and importance of the data or information held in the systems.
- The working environment shall be looked after as one would look after one's own home.

7.2.1 Physical Entry Controls

Units involved in building and facilities management shall control entry and exit to "information technology system areas" so that only authorized "Company employees" may enter and exit, with the following guidelines:

The "Company employees" who are authorized to enter and exit, and the time periods during which they are authorized to enter and exit each "information technology system area", shall be clearly defined.

"Company employees" will be granted rights to enter and exit the workplace only in the areas designated for their work.

If any person who is not a "Company employee" requests entry to an area without having requested access rights in advance, the unit shall verify the reason and necessity before permitting or refusing temporary entry. Such persons shall present a national identification card or other government-issued identification card, and the unit owning the area shall record the person and the entry request as evidence (whether entry is permitted or refused). Entry to and exit from the operations centre by third parties shall be recorded on every occasion, and such records shall be retained for at least 1 year.

Third parties shall exchange their government-issued identification, for example national ID card, driving licence, passport, etc., for the unit's visitor card before being permitted to access the area.

Company employees and third parties shall wear a staff badge or visitor card at all times while on Company premises. Identification cards and visitor cards may not be transferred or lent to others.

Company employees shall never leave Company doors open or allow other persons to follow them into the area (tailgating), unless such persons can present an identification card or visitor card, in order to prevent unauthorized persons from accessing Company premises and security-controlled areas.
Users shall notify security personnel immediately upon seeing strangers or persons not wearing a staff badge or visitor card in the area.
Company employees should accompany, supervise and guide their visitors at all times while the visitors are in the area.

7.2.2 Securing Offices, Rooms and Facilities

Other security measures shall be provided for the Company's offices, rooms and facilities. For example, highly important computers or systems shall not be located in areas with heavy foot traffic; offices or rooms shall not display signs or symbols indicating the presence of important systems within them; doors and windows of offices or rooms shall always be locked when unoccupied; fax machines or photocopiers shall be placed separately from areas that require security; etc.
Staff should check the security of their work areas every day after work to ensure that safes, filing cabinets, drawers and equipment are properly locked and that keys are kept securely.
Information, media, materials and equipment storing confidential information shall never be left unattended on desks, in meeting rooms or in unlocked cabinets.
Information, media, materials and equipment storing confidential information shall not be discarded in waste bins without being appropriately destroyed. The methods of destroying such information, media, materials and equipment shall follow the procedure document on destruction.
Employees shall never allow anyone to remove computers or data storage media from their work area, unless that person is a staff member authorized to do so and the action is carried out under a proper instruction from the department.

7.2.3 Protecting against external and environmental threats

Physical protection against natural disasters, attacks or intrusions, or accidents shall be designed and implemented as follows:

- An emergency alarm system for fire and flood is in place.
- Fire-fighting equipment conforming to standards is in place.
- Air-conditioning and humidity control systems are in place.
- Plans, manuals, drills and post-drill reviews for protection against external and environmental threats.
- A plan for using a Disaster Recovery Site or backup computer systems when an environmental disaster occurs is in place.

- Where an alert is received from a government agency through the system that sends emergency messages to all mobile phones in the target area, Cell Broadcast (CBS), it shall be strictly followed, and coordination shall be made with the Company's business continuity management team.

7.2.4 Working in secure areas

7.2.4.1 Procedures for working in areas requiring security

- Work performed and inspections of work performed shall be reported to ensure that work is correct, complete, in accordance with policies and work procedures, and within the defined scope of authority, duties and responsibilities. In addition, where information technology support services are obtained from third parties outside the Company, there shall be a sufficiently careful and rigorous system for monitoring the work of third parties, such as inspecting the third parties' work records (log files) and requiring third parties to report on their work, etc.
- Each department shall control the work of external parties within controlled areas, for example by not permitting photography or video recording in those areas, etc.
- Departments shall display signs stating "No entry without permission", "No photography or video recording" and "No smoking" within controlled work areas.

7.2.5 Delivery and loading areas

Departments shall restrict the areas accessible to third parties who may enter the premises. Where possible, work-related areas should be separated from areas accessible to third parties; for example, storage and dispatch areas for goods shall not be located in areas accessible to third parties.
Staff and staff of external organizations (Third Party) shall wear identification badges at all times while performing duties in the area, and anyone who sees a person not wearing an identification badge has a duty to notify security personnel immediately.

7.3 Equipment Security

To prevent unauthorized use of computer equipment and to ensure that computer equipment is adequately protected against natural disasters, theft and other damage.

7.3.1 Equipment siting and protection

Equipment maintenance shall be scheduled at the intervals recommended by the manufacturer; maintenance instructions recommended by the manufacturer shall be followed; records of every equipment maintenance activity for services shall be kept for later inspection or

evaluation; and records of equipment problems and defects found shall be kept for use in evaluating and improving such equipment.

The work of external service providers performing maintenance on equipment within the department shall be controlled and supervised.

Access rights to equipment containing important data by external contractors (performing equipment maintenance) shall be approved, to prevent unauthorized access to data.

Areas for installing important equipment shall be allocated so that they are difficult to access.

Equipment shall be installed in enclosed equipment cabinets.

7.3.2 Supporting Utilities

Equipment shall be protected from power failures and other disruptions caused by failures of supporting utilities. Maintenance shall be provided for the relevant utility equipment, such as Uninterruptible Power Supply (UPS), humidity detectors, smoke detectors, etc., and the service of such equipment shall be inspected at least twice a year. Examples of risk-level classification are as follows:

- High risk: shall have backup power systems, both UPS and generator.
- Medium risk: shall have a UPS backup power system.
- Low risk: a backup power system is optional.

7.3.3 Cabling Security

Protection shall be in place for electrical wiring or cables entering the Company's buildings. In areas where electrical wiring or cables enter the Company's buildings and where cable termination cabinets are installed, such cabinets shall be kept locked at all times and access shall be restricted to authorized employees or persons only.

- High risk: cabling shall use cables that are protected against signal interference and against access to the signal cables.
- Medium risk: cabling shall be protected against access to the signal cables.
- Low risk: ordinary signal cables may be used.
- There shall be an inspection plan for the electrical wiring, cabling and communication cabling systems.

7.3.4 Equipment Maintenance

Equipment shall be correctly maintained to ensure its continued availability and correct operation. Maintenance is divided by risk level as follows:

- Systems with high risk shall be maintained every 1 month.
- Systems with medium risk shall be maintained every 3 months.

- Systems with low risk shall be maintained every 12 months.

7.3.5 Removal of Assets

Information equipment or software shall not be taken off the Company's premises without authorization. Anyone wishing to take such items off the premises shall notify their supervisor or the person with authority to grant permission, and shall comply with the applicable procedures.

7.3.6 Security of Equipment and Assets Off Premises

Assets used outside the Company's premises shall be secured, taking into account the risks of working outside the Company's premises.

Secure disposal or reuse of equipment: Equipment containing storage media shall be checked to ensure that any important data and licensed software have been securely deleted or overwritten before the equipment is disposed of or reused.

Unattended user equipment: Users shall appropriately protect equipment that is left unattended in a location for a period of time.

7.3.7 Clear Desk and Clear Screen Policy

For paper documents and removable storage media, and for the protection of information on information processing facilities, when they are taken for use, a request for permission to use them shall be submitted, specifying the start date of use, the date of return, and how they will be stored during the period of use.

8. Technological Control (Annex 8)

Objective

The Company defines and enforces technological controls so that the protection of the Company's information systems, networks, equipment and data is effective and auditable. These controls aim to reduce the risk of unauthorized access, use, disclosure, modification or destruction of data, and to reduce the likelihood of system disruption, in order to maintain the confidentiality, integrity and availability of data and information services. They also support compliance with Company policies, applicable laws and requirements, and support monitoring, detection and retrospective review for the appropriate management of information security events.

8.1 Mobile Device Policy

- Personnel of the Company should be aware of the need to protect and look after portable communication devices, both physically and in terms of the important data stored on them. Physically, devices shall be locked to a desk or stored in a lockable cabinet. Important data stored on the device shall be protected against access by unauthorized persons, which may

be achieved by encrypting the important data on the device, and important data on the device shall also be backed up regularly.

- Personnel of the Company shall obtain permission before connecting their own portable communication devices, such as laptop computers / notebooks / tablets / smartphones or other mobile communication devices, to the Company's network. They should also be aware and exercise caution when the Company's portable communication devices are connected to external networks. The Company sets out the following guidelines for computer use:

Computing devices and/or mobile devices of the Company are Company assets and shall be used for the Company's business operations only.

When returning computing devices and/or mobile devices of the Company, or sending them for repair, the data on them shall be backed up to the designated location or securely deleted in accordance with the confidentiality level of the data on the device.

Users are prohibited from changing or modifying the configuration or components of the Company's computing devices and/or mobile devices without authorization.

The Company's computing devices and/or mobile devices shall not be used for unintended purposes, and use of computing devices and/or mobile devices in environments that may adversely affect the devices shall be avoided.

If it is necessary to use a personal computing device and/or mobile device to connect to the Company's internal network or to access internal systems, approval shall be obtained from the supervisor, and the user shall explain to the supervisor the reason why the personal device needs to be used. The device shall be registered with the Company so that it can be inspected and have the necessary software installed, including the antivirus software purchased and used internally by the Company, and the user shall comply with the usage procedures defined by the Company.

Personal computing devices and/or mobile devices shall be used to access the Company's general business systems only.

Personal computing devices and/or mobile devices shall not be used to access the Company's service management systems.

8.1.1 Unattended User Equipment

- Users shall prevent unauthorized persons from accessing unattended information technology equipment, computers and network systems.
- Users shall log out of information systems and shut down their computers immediately after completing their daily work.

- Computer system administrators shall configure computers to activate a password-protected screen saver every 15 minutes, or to lock the screen when not in use.

8.1.2 Privileged Access Rights

User accounts with high-level access rights to information systems, such as Root or Administrator or equivalent, shall be assigned to personnel only on a need basis and with an access period appropriate to the work.

Where it is necessary to grant high-level privileges to operators or third parties, this shall be carefully considered and tightly controlled, taking the following factors into account:

- Agreement and approval shall be obtained from the owner of the information system concerned.
- Use shall be strictly controlled, for example by permitting use only when necessary.
- A usage period shall be defined, and use shall be suspended immediately when that period expires.
- The password shall be changed after use is completed.

8.1.3 Information Access Restriction

Use of information in information systems shall be controlled, including defining usage rights (e.g. write, read, delete), defining the groups of users permitted to use it, and verifying that the information users are permitted to use is limited to the data necessary for their work.

User accounts with special-level access rights to information systems, such as Root or Administrator, shall be assigned to users only on a need basis and with an access period appropriate to the work.

Third parties shall express their consent to strictly comply with the Company's Information and Communication Technology Security Policy (IT Security Policy) before being permitted to access information technology systems.

8.1.4 Access Control to Program Source Code

Information system developers shall ensure that access to the source code of production or in-service systems is controlled, for example:

- Source code should not be stored on production machines and shall be stored in a secure location.
- Source code under testing shall not be stored together with source code that is already in production use.

8.1.5 Secure Authentication

Secure log-on features or methods should be defined. When a new system is approved for procurement and installation, features such as the following should be considered:

- Not displaying the system name or system details until log-on has succeeded;
- Not providing or not displaying a help option (Help Menu) during log-on;
- Recording each successful or failed log-on by users (for later review);
- Not displaying the password on screen while users enter their password.

8.1.6 Capacity Management

This provides guidance for managing the system resources of services so that they are sufficient to meet service level agreements and to serve the Company's visitors and users, both now and in the future.

The responsibilities of data custodians are defined.

The review and assessment of system capacity is planned, and the maximum acceptable capacity thresholds are defined for both computer equipment and network systems, assessing at least CPU, RAM, Storage and Network Utilization.

The review and assessment of system capacity is carried out as specified above.

System performance is analyzed and processed to identify causes, problems and systematic remedies, and requirements are monitored, improved and forecast for future needs so that systems remain efficient.

The results of system capacity management are summarized.

8.1.7 Separation of Development, Testing and Operational Environments

Information processing facilities (computer systems and networks) used for development and testing shall be separated. For example, in software development, machines used for development and testing should be separated from production machines and, where necessary, the development network should also be separated from the production system.

8.2 Protection from Malware

8.2.1 Control Against Malware

Client computers and portable computers shall have the latest version of antivirus software approved by the Company installed, and it shall be enabled at all times while the machine is in use.

Server computers that provide antivirus services shall always be kept updated with the latest patterns (Update Latest Pattern). All servers, desktop computers and notebooks shall receive the latest updates from the antivirus server.

The configuration documentation of antivirus servers shall be reviewed every 6 months, and a checklist document shall be prepared to support the review.

Employees are prohibited from downloading shareware (trial versions) or freeware directly from the Internet without approval. After approval, staff shall scan the software with antivirus software before use.

All files downloaded within the organization, whether email attachments, copies from disks, or shared files, shall be scanned for viruses.

Users are prohibited from creating, storing or distributing any malicious programs, such as viruses, worms, Trojan horses, email bombs, etc., into the Company's computer systems.

Users are prohibited from obstructing or interfering with the operation of antivirus software.

Only work-related files are permitted to be sent and received via the Company's network. Users should receive files only from persons they know and through plausible communication channels. In addition, users shall always scan received files for viruses with the Company's antivirus software before opening them.

Internet connectivity shall be disabled on all server computers except where it is necessary, to prevent malware from affecting important data on these servers.

Controls against malware: Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware software shall be configured to update the software and its signatures daily.

8.2.2 Management of Technical Vulnerabilities

To secure the software of information systems, including the information in those systems, and to reduce the risk of attacks exploiting technical vulnerabilities that have been published or disclosed in various places:

Information on vulnerabilities in the systems in use is monitored, the risks of those vulnerabilities are assessed, and countermeasures are defined to reduce such risks.

Security-related software shall be regularly kept up to date to close vulnerabilities, and the list of software installed on client computers shall be defined and restricted.

8.2.3 Technical Compliance Review

Technical details of systems in use or in service shall be reviewed at defined intervals to determine whether information security and technology services are adequate. This includes checking whether systems can be intruded upon and whether system parameter configurations are secure, as well as checking systems using vulnerability scanning software (Vulnerability Scanning) and penetration testing (Penetration Test) to identify system weaknesses.

8.2.4 Configuration Management

The Company shall manage the entire lifecycle of security configurations for information technology to ensure an appropriate level of security and to prevent unauthorized changes. This includes defining configurations, implementing them, monitoring them and reviewing them.

The Company has established processes for proposing, reviewing and approving security configurations, as well as processes for managing and monitoring configurations. All configuration changes shall be reviewed at least once a year or whenever there is a change.

8.2.5 Information Deletion Control

Information stored in information systems, devices or other storage media should be deleted when it is no longer required, in order to prevent unnecessary disclosure of sensitive information and to comply with the requirements of the Personal Data Protection Act B.E. 2562 (2019) regarding the deletion of information.

When using cloud services, the Company should verify whether the deletion method provided by the cloud service provider is acceptable and, if so, the Company should use it or request the cloud service provider to delete the information. These deletion processes should be automated in accordance with policy where available and applicable. Records should allow the deletion of information to be tracked or verified, depending on the sensitivity of the information deleted.

To avoid unintentional disclosure of sensitive information when equipment is returned to the vendor, sensitive information should be protected by removing storage devices, hard disk drives and memory before the equipment is sent off the Company's premises.

8.2.6 Data Masking

- Data masking should be used in accordance with the Company's topic-specific policy on access control and other relevant topic-specific business requirements, taking applicable laws into account, in order to limit the disclosure of sensitive data, including personally identifiable information, and to comply with legal requirements, the Personal Data Protection Act B.E. 2562 (2019), regulations and contracts.
- Where there is concern about the protection of sensitive data (sensitive personal data), the Company should consider concealing such data using technical measures such as redaction by striking through on documents, pseudonymization (Pseudonymization) and anonymization (Anonymization).
- When pseudonymization or anonymization techniques are used, it should be verified that they are adequate and appropriate. All elements of the sensitive data should be considered so that the treatment of sensitive data is effective. For example, if not

properly considered, an individual may still be identified even though the data that directly identifies the person does not state the name, through the availability of additional information that allows the person to be identified indirectly.

8.2.7 Data Leakage Prevention Control

Measures shall be in place to prevent leakage of data in order to avoid unauthorized disclosure of sensitive data and, if a data leakage event occurs, to be able to detect it in a timely manner. This includes data in information technology systems, networks or other devices.

The Company has defined a process for managing data classification levels, assesses information technology risks, checks for vulnerabilities that could lead to data leakage, and has data protection measures in place.

8.2.8 Information Backup

The frequency of backups shall be defined based on the importance of the data and the risk acceptance defined by the data owner.

Backup equipment or systems shall be maintained so that they are effective and available at all times.

There shall be physical access control (Physical Access Control) for the locations where backup data is stored. Storage media shall be protected in line with the importance level of the information system.

Backup periods shall be defined according to the level of risk management.

There shall be backup and recovery processes for every system, which shall be documented and reviewed periodically.

A register shall be maintained recording each backup and each data restoration.

Backup data shall be tested periodically to ensure that the backed-up data can be fully restored.

The logging of storage media kept at the storage location shall be reviewed annually.

The process for transferring data between the computer system site and the data storage site shall be reviewed at least once a year.

Storage media shall bear labels showing details, including at least the following:

- System name
- Creation date
- Importance level of the data
- Contact details of the data custodian
- Media retention method, e.g. online backup / hard copy

8.2.9 Redundancies

Availability of information processing facilities:

Systems/processes are prioritized, the relationships between systems are identified, and the recovery time for each system is determined through risk assessment (Risk Assessment) and/or business impact assessment of core processes.

Scenarios or problem severity levels are defined.

Detailed problem resolution procedures are in place for each scenario.

Responsible staff and decision-making authorities are designated.

Details of the equipment required in an emergency for each system are specified.

Units serving as backup or data storage units shall also clearly specify the details of the backup computer center.

The contingency plan is regularly reviewed or updated to keep it current (every 6 months), and the contingency plan is kept in a secure location.

The contingency plan shall be tested at least twice a year, and the tests shall simulate real situations.

The contingency plan shall be communicated to relevant persons at all levels only to the extent necessary, and persons without relevant authority or duties should be prevented from learning of it.

When an emergency occurs, details of the incident, the cause of the problem and the method of resolution should be recorded.

8.3 Logging and Monitoring

8.3.1 Event Logging

Abnormal system operations, system errors and information security events shall be logged, stored and reviewed regularly. The methods and periods of retention shall be defined in accordance with the Computer-Related Crime Act B.E. 2550 (2007) and amendments, with the following minimum conditions:

Critical systems shall log at least the following events: log-on/log-off, authentication failures, changes to access rights, access to important data, and configuration changes. Log integrity (Integrity) shall be maintained and access to logs shall be restricted.

System time shall be synchronized (NTP) to ensure accuracy for investigations.

8.3.2 Protection of Log Information

Requirements are defined for protecting the "log information" of the Company's information systems and infrastructure so that it remains complete and accurate (Integrity), is protected from unauthorized access (Confidentiality), and is available when needed to investigate events

(Availability), and so that it supports audits in accordance with ISO/IEC 27001, PDPA and PCI DSS (if applicable). This covers:

- Application systems (Web / Mobile / Backend / API), databases, operating systems, network devices / Firewall / WAF, IAM / SSO, Cloud (AWS)
- DevOps / CI / CD tools related to system releases (e.g. GitHub / GitLab audit logs, pipeline logs)
- Logs stored both centrally (Centralized Logging / SIEM) and on endpoint systems

Classification and minimization of sensitive data in logs

1. Logs shall be classified according to the Company's data classification.
2. The following data shall not be recorded in logs unless necessary:
   - Passwords / PIN codes
   - Card data (e.g. full PAN), CVV/CVC or SAD as defined by PCI DSS
   - Secrets / keys / tokens that can be used to access systems
3. If unavoidable, masking / redaction (e.g. displaying only part of the value) shall be used and access rights shall be strictly restricted.

Access Control & Segregation of Duties (SoD)

1. Access to log storage systems / log search tools shall follow the principle of least privilege, with clearly defined roles (role-based), such as:
   - Viewer (read-only)
   - Analyst (search/investigate)
   - Admin (manage the logging system)
2. Personnel with rights to "modify / delete / change log settings" shall be limited to approved administrators only, and their duties shall be segregated from those of system developers/users where appropriate.
3. Access shall use individual accounts and MFA, and access rights shall be reviewed periodically (e.g. quarterly / semi-annually depending on risk).

Protection of Log Integrity (Integrity / Anti-tampering)

1. Logs sent to the central system shall be protected against modification/falsification using at least one of the following approaches:
   - Append-only / immutable storage (e.g. WORM or Object Lock)
   - Hashing/signatures/chaining so that modification can be detected

2. The ability to "delete logs" shall be restricted or disabled for general users, and deletion shall be possible only through an approved process with supporting evidence.

Encryption and Secure Transmission (Confidentiality)

1. Logs shall be transmitted over secure channels (e.g. TLS) from their source to the storage system.
2. Stored logs shall be encrypted (encryption at rest) in accordance with Company standards, especially logs containing personal data/important data or that are within PCI scope.
3. Encryption keys shall be managed through an organization-approved key management system, with restricted access.

Retention and Secure Disposal

1. Log retention periods shall be defined by system type/regulatory requirements/risk, in line with PDPA.
2. Internet usage logs: retention of at least 90 days (for audit in accordance with relevant requirements).
3. Security/audit logs of critical systems: retention of 1 year, for retrospective investigation of incidents.

Availability / Backup

1. Log storage systems shall have resilience/backup appropriate to the importance of the system (e.g. replication/backup).
2. Log restoration (log restore) shall be tested at defined intervals to ensure the logs can actually be used for investigations.

Monitoring & Alerting

1. Use cases for detecting anomalies shall be defined, including at least:
   - Large numbers of failed logins, brute force
   - Privilege escalation / role or policy changes
   - Changes to logging configuration / disabling of logging
   - Abnormal access to sensitive data
2. Alerts for significant events shall be sent to the responsible teams (SOC/IT/InfoSec) and linked to the Incident Response process.

Personal Data Protection in Logs (PDPA)

1. Logs are considered data that may identify individuals (e.g. user ID, IP, device ID); access shall be controlled and logs shall be used only for their intended purposes.
2. Logs shall not be used beyond security/audit/operational purposes unless approved through the defined process.

3. Measures shall be in place to prevent unnecessary disclosure (masking, field restriction, restriction of who has access).

Requirements for service providers / third parties: If contractors / service providers access logs or logging systems, they shall:

- Obtain written approval;
- Be granted temporary / task-based rights only;
- Have their activities logged, with rights revoked immediately upon completion of the work;
- Be bound by these requirements in the contract / NDA / DPA (where personal data is involved).

Enforcement and Exceptions

- Violation of this policy may result in disciplinary/contractual action.
- Exceptions shall be documented, stating the rationale, duration and compensating risk controls, and shall be approved by the authorized persons (System Owner + InfoSec).

8.3.3 Administrator and Operator Logs

Activities of system administrators and operators shall be logged, and such logs shall be protected and reviewed regularly.

8.3.4 Monitoring Activities

- The Company has processes for reviewing and assessing the operation of the internal control system established by each unit, to ensure it is at an appropriate level and meets internal control objectives efficiently, effectively and economically, and that it is updated to reflect current circumstances.
- Networks, systems and applications should be monitored for anomalous behavior, and appropriate action should be taken to evaluate potential information security incidents, and to detect anomalous behavior and potential information security incidents.
- The scope and level of monitoring should be defined according to business and information security requirements, taking into account relevant laws and regulations. Monitoring records should be retained for the defined retention period.

8.3.5 Clock Synchronization

All types of systems shall synchronize their time only from time sources designated by the Company, such as the organization's internal NTP server or approved cloud time services.

A standard organizational time zone (e.g. Asia/Bangkok) shall be defined consistently across all systems, and general users are prohibited from changing the time themselves.

Critical/security-related systems (e.g. AD/Directory, SIEM, Firewall, VPN, EDR, Database, critical applications) shall be configured to synchronize time automatically and continuously, and their synchronization status shall be monitored.

Backup time sources (Redundancy) of at least 2 sources / 2 servers (Primary / Secondary) shall be defined to cover failure of the primary time source.

Access to time settings and NTP configuration shall be restricted to authorized persons (Administrator) only, and changes shall be recorded through the Change Management process (except in emergencies).

Monitoring/alerting shall be in place for time drift exceeding the defined threshold (e.g. more than X seconds/minutes as defined by the Company for each type of system), and corrective action shall be taken within the defined timeframe.

When using cloud systems, the cloud service provider's guidelines shall be followed, and the organization's time standard shall be defined consistently with the Company's log/monitoring records.

8.3.6 Control of Operational Software

Installation of software on operational systems:

The installation of software on operational systems is analyzed and planned to prevent the risk of impacts from software installation on operational systems that may result in failure.

There are procedures for controlling the installation of software on operational systems, which shall be followed accordingly.

The results of software installation are summarized, analyzed and evaluated to drive improvements in software installation planning.

8.3.7 Restrictions on Software Installation

The Company shall comply with copyright requirements in the use of intellectual property acquired by its units and shall take care not to infringe them.

The Company shall strictly comply with the requirements specified in software licenses (Software Copyright) and shall control the use of software in accordance with the licenses obtained, including keeping evidence of ownership of licenses when registering software for use, and regularly checking whether installed software is properly licensed.

Users are strictly prohibited from using, copying or distributing any images, songs, articles, books or documents in a manner that infringes copyright, or installing pirated software on the Company's information technology systems.

To ensure that Company staff do not infringe copyright unintentionally or inadvertently, no copies should be made of any software installed on the Company's computers for any purpose without authorization, and likewise no programs should be installed on the Company's computers without authorization, in order to ensure that there is a license covering such installation.
The Company requires computers to be inspected at least twice a year to check the list of software on each computer and to ensure that the Company holds a license for each software product on the computer. If unauthorized software is found, it will be removed and, if necessary, the office may consider substituting other properly licensed software for it.

8.4 Network Security

8.4.1 Network Control

- Network administrators shall restrict access to the network and to information technology systems connected to the network, so that network users can access information technology systems only through an authentication system.
- Network administrators shall perform security testing every time a connection is to be made to a third party's network, to ensure there is no unauthorized access to resources.
- The network administrator shall ensure that no services are opened on the network without authorization.
- Access to network devices for inspection and system configuration, both physical and remote, shall be controlled and may be performed only by authorized network administrators.
- In cases where temporary access rights must be granted to third parties:
- The network administrator shall ensure that there is a person who supervises and monitors such access, and shall revoke the access rights immediately upon completion of the work.
- The network administrator shall inspect and close unused ports on network devices.
- For network services provided by server computers, the network administrator shall permit only those connection ports (Port) that are necessary for the service.
- The network administrator shall regularly update the security patches of network devices.
- The network administrator shall prepare a network diagram (Network Diagram) containing details of the boundaries of the Company's internal network, and shall keep it up to date at all times.
- Computer traffic data shall be retained in compliance with the law.

8.4.2 Security of Network Services

- Users shall use network services only as permitted by the network administrator.
- Users shall use the network in a manner that does not affect overall network performance, for example, sending/receiving large files, or downloading or uploading large files.
- Users of network devices shall not connect them to the Company's network before obtaining permission from the network administrator.
- Use of the network to commit any unlawful act is prohibited.
- Users shall access the network using only their own user accounts.
- Disclosure of information belonging to other persons or to a department without authorization is prohibited.
- Third parties are strictly prohibited from connecting any computer or device from outside to the computer systems and network. If such use is necessary, appropriate approval shall be requested beforehand on every occasion.
- Users are strictly prohibited from installing any hardware or software related to the provision of network services, for example, Routers, Switches, Hubs, Wireless Access Points, etc., without authorization.

8.4.3 Segregation in Networks

- The group providing information technology services is a network that can be accessed and used by users, such as the intranet system and the electronic mail system.
- The group providing information technology services is a network that is accessed and used by information technology systems, and which shall not be accessed directly by users, such as database systems, Directory Service, Domain Name System (DNS), and Printer Service.
- The group providing services to users is a network that can be accessed and used by users' computers.
- The group providing wireless services to users is a network that can be accessed and used by users' notebook computers, tablets and smartphones.
- The network shall be designed according to the groups of information and communication technology services in use, divided by user groups and information technology system groups into an Internal Zone and an External Zone,

in order to enable systematic control and prevention of intrusion. A network diagram (Network Diagram) shall be prepared, containing details of the boundaries of the internal network and the external network and of the various devices, and shall be kept up to date at all times.

8.4.4 Web Filtering

The Company controls access, filters/blocks and restricts access rights to unsafe or risky websites automatically, since users are unable to know which websites are safe or which are dangerous. The IT Department shall be responsible for reviewing and defining the Web Filtering policy, and shall review the policy at least once a year or whenever there is a change.

Company devices shall be configured to route web traffic through the Web Filtering system, and users shall not be permitted to circumvent web filtering (e.g., changing proxy settings themselves / using bypass tools). For off-site work (Remote work), there shall be an equivalent means of enforcing the policy (e.g., via VPN, an SWG agent, or DNS filtering approved by the organization).

Website/content categories to be controlled

The Company shall "Block" websites/categories that are risky or inconsistent with the organization's use, as defined, including at least the following:

- Malware / phishing / malicious domains / Command & Control
- Websites offering downloads of dangerous or unsafe files
- Illegal or inappropriate content (e.g., pornography, gambling, drugs, violence) according to the organizational context and the law
- Unauthorized Anonymizers / Proxies / VPNs (to prevent circumvention of controls)

The Company may define "Restrict / Allow with warning" for categories that affect work productivity or carry moderate risk (e.g., Streaming / personal Cloud storage / Social media), based on business necessity.

Permitting only necessary use (Allow-list / Exception)

Permission to use blocked websites/services shall be requested through the exception/unblocking request process, specifying the business justification, the duration, and the system owner/person responsible.

Exceptions shall be approved in accordance with the line of authority (e.g., supervisor + IT Security), and compensating risk measures (Compensating controls) shall be defined as appropriate.

The Company reserves the right to revoke an exception when a risk is found or when the use is not in accordance with its intended purpose.

HTTPS inspection / personal data protection

Web filtering shall take into account privacy and relevant legal requirements (e.g., PDPA), and shall be used only to the extent necessary for security.

If SSL/TLS Inspection (decryption for inspection) is performed, it shall be approved by the relevant departments, and exceptions shall be defined as appropriate for sensitive data/services that should not be

decrypted (e.g., health/banking categories/specified services). In addition, access to data obtained from the inspection shall be strictly controlled.

Logging & Monitoring

The Web Filtering system shall record the data necessary for auditing, such as the user/device, time, URL/Domain, category, allow/deny, and the reason for blocking.

The log retention period shall be defined in accordance with Company requirements/the law, and access to logs shall be restricted to persons with relevant duties only.

High-risk events (e.g., repeated access to phishing/malware websites) shall trigger alerts and be handled in accordance with the Incident Response process.

User responsibilities and enforcement

Users shall use the Internet in accordance with the Acceptable Use policy and shall not attempt to circumvent web filtering.

Violations may result in suspension of use, disciplinary action, or other measures in accordance with Company regulations and the law.

8.5 Use of Cryptography

To ensure that encryption is used appropriately and that the cryptographic process is understood this being a process for transforming ordinary data into a form that the general public cannot read; to read it, one must understand the method of reading and know the matching means of decryption in order to be able to decrypt it and that it is effective in protecting the confidentiality, authenticity (against forgery) or integrity of information; and to define guidelines for data encryption so that information systems maintain the confidentiality of data and the authentication of information system users, and/or effectively and appropriately protect data from modification by unauthorized persons.

8.5.1 Cryptographic Controls

The Information and Communication Technology Department shall define data encryption measures and guidelines for selecting data encryption standards, defining user groups appropriately according to the risks that may arise to data at each defined classification level. Where encryption is not possible, access shall be appropriately controlled according to duties and responsibilities.

Regarding management of encryption keys, the Information and Communication Technology Department shall define methods for managing the keys used for data encryption, comprising:

Consideration of whether the types of data groups to be encrypted are consistent with the data classification levels and with the data governance guidelines.

Selection of data encryption, which may be performed in 2 ways, as follows:

- Symmetric: encryption and decryption using the same key (Secret Key)
- Asymmetric: encryption and decryption using a key pair (Public/Private Key)

Each encryption method shall be considered with reference to "Data Encryption Methods", and appropriate algorithms shall be used.

8.5.2 Key Management

Cryptographic keys used for encryption in the Company's internal computer network shall be controlled with respect to key generation, key storage, key changes, and key possession.

8.6 Security in Development and Support Processes

8.6.1 Secure Development Policy

Rules for software development shall be defined, and the policies or requirements established by the Company shall be complied with. For example, software development should take security into account at every stage of development, and developers (Developer) should be capable of preventing vulnerabilities from being found in the programs they develop, and shall be able to remediate any vulnerabilities that are detected.

8.6.2 System Change Control Procedures

- Appoint a working group to oversee system access and establish rules for system access.
- Information system developers shall have a process for controlling changes to and modification of software for information systems that are in production or already in service, for example:
- Change requests shall come from authorized persons.
- Requests shall be approved by an authorized person.
- Side effects that may occur after the modification shall be controlled.
- Upon completion of the modification, it shall be accepted by an authorized person.
- Details of the requests shall be retained, etc.

8.6.3 Technical Review of Applications after Operating Platform Changes

The system shall be tested every time there is a structural change. When the operating system is modified or changed, information system developers shall review and test the software in use to ensure that there is no impact on operations and security.

8.6.4 Restrictions on Changes to Software Packages

Vendor software shall be modified via the firewall, and firewall updates shall be set to Manual. When software packages are used, changes shall be controlled to the extent necessary, and all changes shall be tested and documented so that they can be applied when the software is updated in the future.

8.6.5 Secure System Engineering Principles

- An order shall be issued establishing a system security committee. To achieve security in system engineering, [principles] shall be defined in writing, continuously improved, and applied to system development work.
- Prepare engineering architecture blueprints that can accommodate future modifications.
- Review, improve, modify and test the system at every point, and distribute the design to the central unit.

8.6.6 Secure Development Environment

- Appoint a committee to study the system development environment.
- Engage a company that meets standards to develop the system.

8.6.7 Outsourced Development

Contractor assessment (Third-party Due Diligence)

Before work begins, the following shall be in place:

- A project Risk Assessment (according to data level / connectivity / impact on airport operations)
- An assessment of the contractor's security capabilities, such as Secure SDLC, vulnerability management, and incident response
- If PCI DSS is involved, the PCI scope and the contractor's role (service provider/third party) shall be clearly confirmed
- Minimum documents to be requested: security policy/SDL practice, list of personnel with access, sample Pentest/VA reports (may be redacted), preliminary IR plan

Requirements in the TOR/SOW and contract (required for every engagement)

The contract shall specify at least:

- The scope of data the contractor may access / purpose / duration
- Prohibition on using real data in dev/test unless approved in writing and masking/anonymization is applied
- Secure SDLC & Secure Coding with reference to OWASP (Top 10/ASVS as appropriate)
- Vulnerability Fix SLA and a "no go-live to production" criterion if severe vulnerabilities remain
- Incident/Breach Notification: notification timeframe (e.g., within 24 hours after an incident is found/suspected) and cooperation in investigations
- Audit right, including the right to request evidence of controls/test reports

- Subcontractor control: subcontracting without approval is prohibited, and subcontractors shall be bound by the same requirements
- IP Ownership & Deliverables: source code, IaC, documentation, runbook, test evidence, pipeline
- Maintenance/SLA: response time, patching, on-call, incident support

Access Control for GitHub/GitLab and AWS

- Use individual accounts only; account sharing is prohibited.
- Enforce MFA for GitHub/GitLab, AWS IAM/SSO and all critical tools.
- Granting of access rights shall be approved and shall follow the principle of Least Privilege + time-bound access where appropriate.
- Permanent access keys shall not be used unless necessary; SSO/role assumption shall be used as the primary method.
- There shall be a Joiner–Mover–Leaver procedure: add/change/revoke access rights immediately upon a change of duties or termination of the contract.
- Production access shall be limited to cases of necessity, logged, and approved on a case-by-case basis (break-glass).

PDPA-specific requirements (personal data)

- A DPA (Data Processing Agreement) shall be prepared, specifying the roles (controller/processor), purposes, security measures, retention period, and deletion/return of data.
- Transfer/disclosure of personal data to other persons without approval is prohibited.

Handover and termination of contract (Exit)

Upon completion of the project / termination of the contract:

- Hand over source code, IaC, pipeline, architecture documentation, runbook, admin manual, and test reports
- Transfer ownership of repos/projects and close/revoke all of the contractor's access rights
- Return/delete Company data and issue a certificate of data deletion/destruction (upon request)
- Conduct knowledge transfer to the internal team

8.7.8 System Security Testing

Requirements of which at least 2 items shall be included in the testing:

- SAST/SCA/Secret/IaC/Container scan: every time in CI/CD (at least every PR/every build)
- DAST: at least per release or monthly (according to risk)

- Vulnerability scan (infra): at least monthly and after major patch cycles
- Penetration test: at least once a year for high-risk/publicly exposed systems, and every time after a major change
- PCI DSS (if applicable): follow the frequency/requirements of PCI in the relevant parts (e.g., testing/scanning according to the criteria of the standard)
- "Pass before go-live" criterion (Go-Live Security Gate): a system may go into Production only when:
- Critical/High vulnerabilities = 0 (or written Risk Acceptance has been approved by an authorized person)
- There is evidence of remediation and re-testing for significant issues
- The necessary Logging/Monitoring has been enabled (including an audit trail of access to important data)

8.7.9 System Acceptance Testing

- A test plan or relevant criteria for system acceptance shall be prepared, for both new systems and modified systems.
- Acceptance criteria shall be established for new systems, procured systems, or other information resources before use. In addition, a checklist document of the items tested shall be prepared before the system is accepted, signed by the officer conducting the tests and by the person delivering the system.

8.8 Test Data

8.8.1 Protection of Test Data

Real data to be used for system testing shall first be authorized by the person responsible for safeguarding that data. Upon completion of use, the real data shall be deleted from the test system immediately, and a record shall be kept as evidence of which tests the real data was used for, including the date, time and the department that performed the testing, and the person responsible for safeguarding that data shall be notified again.

8.9 Change Management

8.9.1 Change Management Policy

- Before making any change to information technology systems, network systems, computer systems, software or databases, the system administrator or external service provider shall request approval for the change from the IT Department in writing.
- Changes to network systems, computer systems, software or databases by external service providers shall be supervised by the information technology system administrator.
- The information technology system administrator shall notify users every time before making a system change.
- The information technology system administrator or external service provider shall assess the impact of a system change before making the change, in order to prevent impact on the operation of systems currently in use.
- The information technology system administrator shall record the details of changes to information technology systems.
- The information technology system administrator or external service provider shall always test the change beforehand, especially in the case of critical information technology systems.
- The information technology system administrator or external service provider shall define a Fallback Plan in case the change does not proceed as expected.
- The information technology system administrator or external service provider shall define a period for monitoring the change in order to check for any impact that may occur on the system after the change.

8.9.2 System Change Control Procedures

- Information system developers shall have a process for controlling changes to and modification of software for information systems that are in production or already in service, for example:
- Change requests shall come from authorized people.
- Requests shall be approved by an authorized person.
- Side effects that may occur after the modification shall be controlled.
- Upon completion of the modification, it shall be accepted by an authorized person.
- Details of the requests shall be retained, etc.

8.9.3 Technical Review of Applications After Operating Platform Changes

When the operating system is modified or changed, information system developers shall review and test the software in use to ensure that there is no impact on operations and security.

8.9.4 Restrictions on Changes to Software Packages

When software packages are used, changes shall be controlled to the extent necessary, and all changes shall be tested and documented so that they can be applied when the software is updated in the future.

9. Legal Compliance and Regulatory Requirements

The Company continuously conducts security audits to ensure accuracy and conformity with policies, regulations and laws.

Compliance with policies and regulations

All employees shall strictly comply with this information security policy and the documents related to this policy, as well as other related policies, such as the Personal Data Protection Policy. Any employee who neglects, or intentionally fails, to comply shall be deemed to have violated such policies and shall be subject to penalties, which may be as severe as dismissal.

Compliance with laws and regulations

The information security policy shall be in accordance with legal requirements, such as the Personal Data Protection Act B.E. 2562 (2019) (PDPA), and laws relating to data protection, data access, privacy protection, and electronic documents, etc.

Under the regulations of the Computer-Related Crime Act B.E. 2550 (2007), the Company is deemed to be an Internet access service provider and shall therefore record and retain all Internet traffic data, by date and time of access, for at least 90 days or longer.

10. Regulations and Penalties

10.1 Any act suspected of violating the security policy (hacking, destruction of data by computer viruses), or any suspected intrusion into or interference with information systems, shall be reported to management and the information security officer immediately.

10.2 Any act suspected of violating personal data shall be reported to the Data Protection Officer immediately, with reference to the "Personal Data Protection Policy".

10.3 Violation of, or non-compliance with, the information security policy shall carry severe penalties for the violator. The severity of disciplinary penalties depends on the act and may be as severe as dismissal.

10.4 Compliance with regulations by all employees is under the supervision of the head of department or a person of higher rank. When an employee commits an offence or violates the rules, the head of department or a person of higher rank shall consider the penalty.

10.5 The following acts are deemed violations of the rules:

10.5.1 Changing or modifying data in the system without prior authorization from an authorized person or supervisor.

10.5.2 Forging or stealing usernames and passwords to access any application system, whether intentionally or unintentionally.

10.5.3 Using another person's user account and password to access a computer system to read, copy or duplicate, change or delete data, for any reason whatsoever.

10.5.4. Negligently allowing another person to use one's own user account and password to access a computer system, including allowing them to use one's access rights to such computer system.

10.5.5 Attempting to disclose, sell or distribute the Company's information.

10.5.6 Attempting to access any system or application without the right to use it.

10.5.7 Installing, examining, monitoring or using hacking tools or programs related to computer system security testing, except by people whose duties include such activities.

10.5.8 Setting up or changing a computer's address (IP address) without prior authorization from the Information Technology (IT) Department.

10.5.9 Changing, relocating or installing any part of a computer system without prior authorization from the IT Department.

10.5.10 Colluding with third parties to allow them to use the computer systems or any application program, or to undermine the security of the Company's data or systems.

10.6 Penalties for violation and negligence

10.6.1 Verbal warning

10.6.2 Issuance of a warning letter

10.6.3 Temporary suspension from work

10.6.4 Termination of employment with the Company

10.6.5 The Company shall consider and exercise due care and discretion in penalizing employees who commit offences under or violate this policy.

Conclusion

Pro Inside Public Company Limited needs to develop policies, procedures, guidelines and standards to support the implementation of this information security policy, which has been officially announced for acknowledgement within the Company. The security policy manual may be used as a reference to the standards or sub-policies used to control the various systems within the Company and is continuously improved.

Effective from 26 June 2026 onwards.

-Mr. Wisut Srisuphan-

(Mr. Wisut Srisuphan)

Chairman of the Board of Directors

Approved by the Board of Directors' Meeting

No. 4/2569 (2026)

on 25 June 2026