SUPALAI

Information Technology and Security Policy

Document Number SPL-DT-PC-2601

Version: 00

ประวัติการปรับปรุงเอกสาร

(DOCUMENT VERSION HISTORY)

Revision No.	Effective Date	Revision Details
00	05 Feb 2026	Initial Release

Document Approval

Created by	Reviewed by	Approved by
คุณเฉลิมพล ลีลาชุติพงศ์	คุณมงคล นิตะโคตร	คุณไตรเตชะ ตั้งมติธรรม
ผู้จัดการแผนก Digital Infrastructure & Cybersecurity Office (ประธาน ISMR)	ผู้อำนวยการ ฝ่ายดิจิทัลเทคโนโลยี (รองประธาน ISMS Management)	กรรมการผู้จัดการ (ประธาน ISMS Management)
5 / Feb / 2026	5 / Feb / 2026	5 / Feb / 2026

สารบัญ

Rationale 6
Objectives 6
Scope / Applicability 6
Definitions 7
Section 1 : Organization of Information Technology and Security Policy 13
Part 1.1 Organization of Information Security 14
Part 1.2 Asset Management 16
Part 1.3 Access Control 18
Part 1.4 Supplier Relationships 21
Part 1.5 Information security for use of cloud services 22
Part 1.6 Budgeting and Accounting for Services Policy 25
Part 1.7 Service Level Management Policy 25
Part 1.8 IT Insourcing and IT Outsourcing 26
Part 1.9 Information Security Incident Management 28
Part 1.10 Incident and Service Request Management Policy 29
Part 1.11 Information Security Aspects of Business Continuity Management 30
Part 1.12 Business Continuity Management 31
Part 1.13 Compliance 32
Part 1.14 Documented operating procedures 35
Section 2: Human Resource Security Policy 36
Part 2.1 Human Resources Security 36
Part 2.2 Remote working 38
Part 2.3 Reporting Information Security Events 38
Section 3 Physical Security Controls Policy 39
Part 3.1 Physical and Environment Security 39
Section 4: Technological Controls Policy 44
Part 4.1 User Endpoint Device Security Policy 44
Part 4.2 Access Right Management Policy 46

Part 4.3 Operations Security 49
Part 4.4 Data Security Policy 53
Part 4.5 Service Reporting Policy 55
Part 4.6 Communications Security 56
Part 4.7 Use of Cryptography 58
Part 4.8 System Acquisition, Development and Maintenance 59
Part 4.9 Change Management Policy 63
Part 4.10 Protection of information systems during audit testing 64
Section 5: Artificial Intelligence Governance Policy 65
Disciplinary Penalties 65
Annex 1: Supalai Partner Code of Conduct 66
Annex 2: IT and Cyber Security Risk Assessment Form for External Contractors 71

Rationale

Supalai Public Company Limited and its subsidiaries ("the Company") have implemented information technology systems to facilitate operations, enhance efficiency, and improve overall organizational effectiveness. To ensure that the use and delivery of services operate appropriately in alignment with business policies, and to prevent issues that may arise from improper use of information technology network systems, whether by users or through various threats, that could cause damage to the Company's business operations.

Therefore, in order to maintain the Confidentiality, Integrity, and Availability of the Company's information systems, it is deemed appropriate to establish this Information Technology Security Policy as a unified guideline for practice, as follows.

Objectives

1. To define the direction, principles, and framework of requirements for information technology security management.
2. To build awareness and understanding among employees so that they may correctly and appropriately comply with policies, standards, operational frameworks, procedures, guidelines, and laws relating to computer systems.
3. To enable employees and all individuals who are required to use or connect to the Company's computer systems to do so correctly and appropriately.
4. To prevent the Company's computer systems and information assets from being intruded upon, stolen, destroyed, interfered with, or compromised in any manner that may cause damage to the Company's business operations.
5. To protect the Company's assets, databases, and information from both internal and external threats, whether intentional or unintentional, and to maintain the Integrity, Confidentiality, and Availability of information, databases, and electronic data communications in accordance with applicable requirements, regulations, and laws.

Scope / Applicability

This policy applies to all levels of the Company's employees, as well as external parties who have been granted authorization by the Company to access or use the Company's computer systems, information networks, and data. Compliance with this policy is mandatory and shall be strictly observed by all parties.

Definitions

No.	Term	Definition
1.	Company	Supalai Public Company Limited and its subsidiaries
2.	Subsidiary	A company over which Supalai Public Company Limited has controlling authority
3.	ISMS Working Committee	The Information Security Management System Working Committee
4.	Digital Technology Department (DT)	Digital Technology Department (DT)
5.	Department-Level Executive	The most senior executive of each respective department
6.	Authorized Person	A supervisor at the level of Department Director or above, or a person designated with decision-making authority
7.	Administrator	A Digital Technology Department staff member assigned responsibility for maintaining computer systems or networks, including resolving information system issues, with access to programs or computer networks for administrative purposes
8.	Personnel or User	Employees of Supalai Public Company Limited and its subsidiaries
9.	External Party	An individual or employee of an external organization who contacts the Company and has access to the organization's information assets
10.	External Service Provider / Third Party	Traders, business partners, vendors, outsourced contractors, and any other individuals or legal entities, domestic or foreign, that provide information technology services under a contract or service agreement with the organization, including subcontractors engaged by such external service providers
11.	Authorized External Party	Traders, business partners, vendors, outsourced contractors, and any other individuals or legal entities, domestic or foreign, that provide information technology services under a contract or service agreement with the organization, including subcontractors engaged by such external service providers, who are authorized to access the organization's premises or information assets and use the organization's information systems within their designated scope of responsibility
12.	User	Personnel, external parties, and external organizations that use the organization's computer systems
13.	Project Owner	An internal unit of Supalai Public Company Limited or its subsidiaries responsible for managing a project in which an external service provider or third party has been engaged to perform work for the organization

No.	Term	Definition
14.	Asset Owner / Data Owner	The individual, unit, or department that owns the data, or the party that would suffer the greatest loss in the event that the data is damaged or disclosed
15.	Information	Text, messages, documents, audio, or any other meaningful content in the form of numbers, language, images, or symbols that has not yet been processed, whether in electronic or printed form, including computer data as defined under the Computer Crime Act and electronic data as defined under the Electronic Transactions Act
16.	Electronic Data	Messages that have been created, transmitted, received, stored, or processed by electronic means, such as electronic data interchange, email, telegraph, telex, or facsimile
17.	Computer Data	Data, messages, instructions, command sets, or any other content residing in a computer system in a state that the system is capable of processing, including electronic data as defined under the Electronic Transactions Act
18.	User Account	A set of data used to identify a user, define access rights, and establish restrictions for accessing information systems
19.	Password	A set of characters used for authentication to control access to information systems or information assets
20.	Privilege	An elevated level of access rights that exceeds those of a standard administrator or general user, such as Root or Administrator access
21.	Information System	Computer systems, data storage systems, email systems, all types of data communication systems, communication devices, printers, scanners, or any related equipment owned by the organization and/or lawfully licensed for the organization's use
22.	Information Security	The preservation of the Confidentiality, Integrity, and Availability of information, along with other properties including Authenticity, Accountability, Non-repudiation, and Reliability
23.	Information Security Event	An identified occurrence of a system, service, or network state that indicates a possible breach of information security policy, a failure of security controls, or a situation where the security implications are unknown
24.	Incident	A disruption that causes an information system to be unable to deliver services as defined, or results in a degradation of service quality, such as email system unavailability, server failure, or abnormal processing errors

No.	Term	Definition
25.	Data Backup	The process of creating copies of all data in a target system to safeguard against data modification, changes, or loss, enabling recovery and restoration of data
26.	Source of Data and Information	Repositories storing data or information in various forms, such as dedicated data sources and centralized data repositories
27.	Information Security Incident	An unwanted or unexpected information security situation that may result in the organization's systems being compromised or attacked, and security being threatened
28.	Encryption	The transformation of data into a secure format using an encryption key, such that the content cannot be understood without decryption using the correct key. There are two types of encryption: • (1) Symmetric Key Encryption, which uses a single key (Secret Key) for both encryption and decryption; and • (2) Asymmetric Key Encryption (Public Key Cryptography), which uses a key pair consisting of a Private Key and a Public Key, referred to in this policy as a key pair
29.	Key	A key used in the encryption or decryption process, depending on the cryptographic technique employed. There are two types: • (1) Secret Key, used in Symmetric Key Encryption, with examples including 3DES, RC5, RC6, and AES; and • (2) Key Pair, used in Asymmetric Key Encryption (Public Key Cryptography), consisting of a Private Key and a Public Key, with examples including RSA (Rivest-Shamir-Adleman), Diffie-Hellman Key Exchange Protocol, and Elliptic Curve Cryptography (ECC)
30.	Vulnerability	A flaw or weakness in an information asset that may result from deficiencies in production, design, or management, creating weaknesses susceptible to threats, such as a software vulnerability that allows unauthorized external access without authentication
31.	Security Awareness	The provision of knowledge and understanding of information security to personnel, in order to raise awareness of threats and information security risks
32.	Information Asset	Data, information, or technology components of value and importance to the organization's operations, in both electronic and physical form, including computer systems and networks, that must be managed and secured to prevent damage from destruction or leakage, such as IT equipment, software and

No.	Term	Definition
		application systems, data, electronic data, computer data, and intellectual property
33.	Secure Area	An area designated for housing information technology equipment used in information systems, categorized into three types: • (1) IT equipment storage rooms; • (2) computer laboratory areas; and • (3) Data Center rooms
34.	Logs	Records of information system usage events, system access activities, information system processing activities, and security events, used to monitor performance, security, and anomalies arising from information system activities
35.	Monitoring	The surveillance of information security to detect anomalies in information system activities through event logs, such as unauthorized access, misuse of information systems, and system-related issues
36.	Risk	The likelihood of errors, damage, leakage, loss, or undesirable events occurring under uncertain conditions that may impact or prevent the achievement of service objectives and goals
37.	Malicious Code or Malware	Programs or code that are harmful to the performance and security of information systems in any way, such as viruses, worms, or trojans
38.	Business Continuity Plan (BCP)	A plan to ensure business continuity and prevent disruption or interruption to critical business transaction systems, which may be caused by environmental hazards, security incidents, or other threats
39.	Disaster Recovery Plan (DRP)	A preparedness plan for emergency situations, covering responses ranging from relocation of operations to the activation of backup information systems
40.	Fallback Plan	An operational plan used to revert to the most recent stable operating state in the event that emergency remediation efforts are unsuccessful
41.	Recovery Point Objective (RPO)	The maximum tolerable period during which data may be lost from a system, used as a basis for designing data backup methods to ensure data loss does not exceed the defined threshold
42.	Recovery Time Objective (RTO)	The target timeframe within which products, services, activities, or processes must be restored to normal operations following a severe disruption

No.	Term	Definition
43.	Maximum Tolerable Period of Disruption (MTPD)	The maximum duration of an operational disruption beyond which normal operations cannot be restored
44.	Service Level Agreement (SLA)	A mutual agreement between a service provider and a service recipient describing service details, measurable service levels, service level targets, and the clearly defined responsibilities of both parties
45.	Operational Level Agreement (OLA)	An internal service agreement between internal units to support the delivery of services to recipients in accordance with the Service Level Agreement (SLA)
46.	Underpinning Contract (UC)	A mutual agreement between a service provider and a vendor to ensure that services are delivered to recipients in accordance with the Service Level Agreement (SLA)
47.	Development Area	An information system environment used for system development, simulating the resources and environment of the production system for the purpose of improving and developing applications
48.	User Acceptance Test (UAT)	The final phase of system testing conducted prior to deployment to the production environment, performed by end users to verify that the system functions correctly, meets requirements, and delivers a satisfactory user experience
49.	Disaster Recovery Center (DR)	Backup systems, data, and network infrastructure separate from the primary information systems, enabling continuity of core business transactions and minimizing impact during emergency situations
50.	Production Area	The live information system environment serving end users, which must be strictly secured and access-controlled, separate from development and testing environments
51.	Mobile Device	Portable computing devices including laptop computers, smartphones, and tablet computers that the organization has authorized to connect to and use the organization's information systems
52.	Media	Electronic devices used for recording or storing data, such as hard drives, flash drives, handy drives, thumb drives, or external hard drives
53.	Artificial Intelligence (AI)	Technology developed to enable computers to exhibit characteristics or behaviors resembling human intelligence, such as learning, perception and environmental response, reasoning, and problem-solving, in accordance with human-defined objectives

No.	Term	Definition
54	Data Center (DC)	A physical facility established as a centralized hub for storing, processing, and managing the organization's large-scale digital data. It comprises servers, storage systems, and network equipment, supported by high-security infrastructure such as cooling systems, uninterruptible power supplies (UPS), and intrusion prevention measures, operating continuously 24 hours a day

Section 1 : Organization of Information Technology and Security Policy

The Company has established this Information Technology and Security Policy to define the direction, principles, and framework of requirements for protecting information-related assets against threats that may compromise the Confidentiality, Integrity, and Availability of data and information systems. The policy aims to promote robust internal information security controls based on a Risk-Based Approach in alignment with international standards, and to support users and relevant parties in recognizing the importance of information security, as well as understanding their responsibilities and guidelines for managing various risks. The organization shall establish information security policies and measures in accordance with the following guidelines.

1. Information Security Objectives

   The Company has defined objectives aligned with its established information security goals to serve as a framework for key performance indicators, as follows:

   1) To ensure that the organization has implemented information security management measures for its systems in compliance with the Personal Data Protection Act and international standards.
   2) To promote information security awareness and strengthen the capabilities of personnel within the scope of the Information Security Management System.
   3) To undertake corrective actions for any identified non-compliance with information security policies.
   4) To ensure that systems within the scope of the Information Security Management System and the Personal Data Management System maintain Confidentiality, Integrity, and Availability, and are capable of delivering continuous services.
   5) To measure the number of incidents affecting the information technology service delivery within the Information Security Management System.

2. Management Directions for Information Security

   1) Policy for Information Security

      - The organization shall establish a written information security policy for its information systems, approved by the Chairman of the Board of Directors or a senior executive designated by the Chairman as the approving authority.
      - The organization shall disseminate the policy to users and relevant external parties for acknowledgment and compliance. The dissemination shall be carried out in a manner that is easily accessible to users.

2) Policy Dissemination
   - The Digital Technology Department is responsible for announcing and disseminating the policy to users of the organization's information systems, in order to promote understanding of their individual roles in using information technology and protecting the organization's assets.

3) Review of the Policies for Information Technology and Security
   - This Information Technology and Security Policy shall be reviewed and updated at least once a year, or whenever significant changes occur in the operating environment, such as changes in business conditions, regulations, laws, or technology. It is the responsibility of the Digital Technology Department to conduct the review and update, under the oversight of the Digital Technology Department executive, who shall ensure that reviews and updates are carried out as defined.
   - The Digital Technology Department shall conduct inspections and reviews of the Information Technology and Security Policy in accordance with the conditions specified.

Part 1.1 Organization of Information Security

Objective

To establish measures for controlling, governing, and monitoring the performance of information security responsibilities across various units within the organization, and to provide guidelines for the use of mobile devices in compliance with the information security policy.

1.1.1. Internal Organization

1) Information Security Roles and Responsibilities
   - Department-level executives shall define the information security responsibilities of personnel within their respective units in writing, in accordance with the established information security policy. In addition, department-level executives shall ensure that responsibilities relating to information security operations are clearly segregated across all relevant functions (Segregation of Duties), so as to enable mutual review and oversight between parties.

2) Contact with Authorities
    - The Digital Technology Department shall collect and maintain contact information for all parties involved in information security operations, including relevant specialists, and shall review such information on a regular basis. A directory of contacts shall be maintained for coordination with external authorities, including the National Cyber Security Agency (NCSA), the Technology Crime Suppression Division (TCSD), the Office of the Personal Data Protection Committee (OPDPC), and other relevant regulatory bodies. This directory shall be used for coordination purposes in the event that information security incidents occur or when such contact becomes necessary.
3) Contact with Special Interest Groups
    - The Digital Technology Department shall participate in and maintain a directory of special interest groups, information security expert communities, and professional associations, such as the Thai Bankers' Association Computer Emergency Response Team (TB-CERT) and the Thailand Computer Emergency Response Team (ThaiCERT). This is to facilitate access to advice, knowledge, and the sharing and exchange of information relating to technologies, products, services, emerging threats or vulnerabilities, and threat intelligence relevant to critical information systems, for the purpose of enhancing information security practices. The directory of group contacts shall be reviewed on a regular basis.
4) Information Security in Project Management

    Department-level executives shall ensure that risk controls, project progress monitoring, and overall project assessments are implemented for both internal projects and externally procured projects, in compliance with applicable security requirements. Responsibilities and authorities for information security relating to each project shall be clearly defined, covering the following key areas:
    - **Integration of Security into Projects:** From project initiation, potential risks to information shall be assessed and preventive measures planned accordingly.
    - **Training and Awareness:** All project-related personnel shall receive training and be made aware of the importance of information security.

- **Access Control:** Access to information used within the project shall be appropriately controlled to prevent unauthorized access.
- **Risk Assessment and Review:** Information security risk assessments shall be conducted on a continuous basis throughout the project lifecycle.
- **Security Incident Management:** A response plan shall be in place and immediate action shall be taken upon the identification of any security incident occurring during the project.

Part 1.2 Asset Management

Objective

To ensure that the organization's assets and information systems are protected at an appropriate level, in order to reduce the risk of unauthorized disclosure of organizational information, prevent misuse of information assets, and protect against damage to the organization's information assets.

1.2.1. Responsibility for assets

1) Inventory of Assets
   - The Digital Technology Department shall ensure that units within the department maintain an inventory of information assets for the purpose of appropriate management and control, and shall ensure that the asset inventory is kept up to date at all times.
2) Ownership of Assets
   - Supervisors within the Digital Technology Department at level 6.2 and above shall ensure that asset owners, custodians responsible for controlling the use of information assets, and personnel accountable for information assets are appropriately identified and designated.
3) Acceptable Use of Assets
   - Managers of the Digital Technology Department and above shall establish acceptable use requirements for information assets to ensure appropriate management of computer equipment for maximum efficiency and protection against potential damage. Such requirements shall be communicated to all organizational personnel for acknowledgment and compliance.

4) Return of Assets
   - The Human Resources Department, supervisors, or line managers shall oversee and ensure that personnel within their units, as well as external service providers engaged by the organization, return all organizational assets upon separation or completion of services, including but not limited to laptop computers, documents, keys, and employee access cards, to the relevant units.

1.2.2. Information Classification

1) Classification of Information
   - The organization shall establish a framework for categorizing information assets and defining information classification levels, taking into account applicable laws and regulations relevant to the organization when determining appropriate classification levels.
   - Internal units shall categorize data and information assets used in organizational operations and assign appropriate information classification levels.
   - Internal units shall manage information classification levels in accordance with the procedures defined in the Information Security Policy.

2) Labeling of Information
   - The organization shall ensure that information in document form is appropriately controlled and secured throughout its lifecycle, from creation, labeling, storage, copying, and distribution through to disposal. Procedures shall be established and all personnel and relevant parties shall comply, to ensure that information is adequately controlled and secured.
   - The Digital Technology Department and relevant units shall affix asset labels in accordance with the asset inventory register and usage procedures on all computer equipment.

3) Handling of Assets
   - The Digital Technology Department shall control and oversee the establishment of operational procedures for managing information assets, to prevent leakage of the organization's critical information or misuse of information assets.

1.2.3. Information transfer

1) Guidelines or procedures shall be established for the transfer of information through all types of tools or devices, covering both internal information transfers and transfers between the organization and external parties. Information security shall be maintained in accordance with the organization's defined information classification levels, covering the following:
    - Information in use at endpoint devices (In Use / At Endpoint)
    - Information in transit across networks (In Transit)
    - Information at rest within systems and storage media (At Rest), including information stored on devices and storage media

Part 1.3 Access Control

Objective

To establish security guidelines for controlling access to and use of the organization's information systems, and to prevent unauthorized intrusion through network systems, including from malicious programs that may cause damage to the organization's data.

1.3.1. Business Requirement for Access Control

1) Access Control Policy
    - The organization shall establish written access control procedures, keep them up to date at all times, and communicate them to internal users for acknowledgment and compliance.
2) Access to Networks and Network Service
    - The Digital Technology Department shall require that all user requests to access data and information systems be approved by the user's direct supervisor.
    - The Digital Technology Department shall restrict user access to network services solely to those that the user has been authorized to access, and such access rights shall be granted in accordance with the user's responsibilities and operational requirements.

1.3.2. User Access Management

1) User Registration and De-Registration
    - The Digital Technology Department and data owners shall jointly establish written procedures for managing user registration and de-registration, keep such procedures up to date, and communicate them to internal users for acknowledgment and compliance.

2) User Access Provisioning
   - The Digital Technology Department and data owners shall ensure that access rights to data or information systems are assigned to users in accordance with their designated responsibilities.
   - The Digital Technology Department and data owners shall prepare and retain documentation of access right assignments as evidence of operations.
   - The Digital Technology Department and data owners shall define a process for managing access rights in cases where a user requires access to data or information systems beyond their assigned rights.

3) Review of User Access Rights
   - The Digital Technology Department and data owners shall establish written procedures for reviewing access rights to data, information systems, and applications, keep such procedures up to date, and communicate them to internal users for acknowledgment and compliance.
   - The Digital Technology Department and data owners shall define a clear review cycle for access rights to data and information systems, and notify all relevant parties accordingly.
   - Access rights reviews shall take into consideration the following:
     1) The defined access rights review cycle
     2) Separation of personnel from the organization
     3) Changes or transfers of job responsibilities
     4) Requests for access rights beyond the user's defined scope of responsibility
   - Upon completion of each access rights review, the data owner or system administrator shall retain evidence of the review, categorized by review period.

4) Removal of Access Rights)
   - Data owners and system administrators shall establish written criteria and procedures for revoking access rights, and communicate these to internal users for acknowledgment and compliance.

1.3.3. Identity management

The organization shall manage unique identity attributes linked to individual users for authentication purposes, and shall establish processes for securing authentication-related information. Security awareness relating to authentication shall be communicated to personnel to promote appropriate practices, such as refraining from writing usernames and passwords on desks or in locations where unauthorized individuals may gain access to organizational systems.

1.3.4. Use of Secret Authentication Information

1) The organization shall define processes and select appropriate technical methods for authentication, to verify the identity of users. This shall cover the full identity lifecycle including identity creation, modification, suspension, and revocation, ensuring that access to the organization's information and personnel data is granted in accordance with each user's assigned roles, responsibilities, and operational requirements.
2) Password Management System
    - The Digital Technology Department shall provide a system for managing user accounts and passwords for accessing the organization's information systems, to ensure standardized and consistent management practices.
3) User Responsibilities
    - Users shall not use easily guessable password structures or characteristics, such as dictionary words, combinations or derivatives of the username, sequential characters, personal information, or any easily predictable phrases.
    - Users shall not write down or record their passwords and store or display them in proximity to the systems or devices to which those passwords relate.
    - Users shall be accountable for all actions that can be attributed to their user accounts, and shall not permit others to perform any actions using their accounts, nor perform any actions using another user's account without authorization.
    - Users shall comply with all other password management requirements established by the organization.

Part 1.4 Supplier Relationships

Objective

To establish measures for evaluating the use of information technology services from external service providers, including measures for governing, monitoring, and reporting on the performance of such providers, in order to ensure that the use of such services is efficient, secure, and delivers maximum benefit to the organization.

1.4.1. Information Security in Supplier Relationships

1) Information Security Policy for Supplier Relationships
   - The Digital Technology Department shall establish an information security policy governing relationships with external parties. Relevant personnel shall assess potential risks and define mitigation measures before authorizing external parties or individuals to access the organization's information systems or data. System administrators and units designated to liaise with external parties shall ensure that external individuals or organizations providing contracted services comply with the applicable service contracts or agreements, covering security obligations, service characteristics, and service levels.

2) Addressing Security within Supplier Agreements
   - The Digital Technology Department shall ensure that written information security agreements are established in relation to authorizing external parties to access information systems or data for purposes of reading, processing, managing, or developing information systems.
   - System administrators and units designated to liaise with external parties shall ensure that external parties are granted access only to the information strictly necessary for their work, and that such access is approved in writing by the information asset owner.
   - System administrators and units designated to liaise with external parties shall ensure that external parties comply with all requirements and agreements established between the organization and those parties.

3) Information and Communication Technology Supply Chain
    - The Digital Technology Department shall ensure that agreements and responsibilities relating to information security risks are incorporated into contracts with external parties providing information and communication technology services, including subcontractors engaged by those external parties.

1.4.2. Supplier Service Delivery Management

1) Monitoring and Review of Supplier Services
    - System administrators and units designated to liaise with external parties shall regularly monitor and review the performance of external parties responsible for managing the organization's information processing systems, covering their financial standing, operational processes, and service delivery effectiveness.
2) Managing Changes to Supplier Services
    - In the event that an external service provider makes changes to its processes, procedures, operational methods, or operational security practices, system administrators and units designated to liaise with external parties shall conduct a risk assessment of such changes, report the findings to management and relevant stakeholders, and define appropriate risk management processes in response.

Part 1.5 Information security for use of cloud services

Objective

To establish principles, measures, and information security requirements for the organization's use of cloud services, in order to ensure that the use, storage, processing, and management of cloud services are secure and compliant with applicable laws, standards, and the organization's information security policies.

1.5.1. Cloud Provider Selection & Assessment

1) The organization shall conduct security assessments of cloud service providers, evaluating their reliability and compliance with international standards such as ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018, and shall perform risk assessments prior to initial use and whenever significant service changes occur.
2) The organization shall verify the appropriateness of SLA terms, availability commitments, backup provisions, recovery capabilities, and security responsibilities before entering into contracts or commencing use of any cloud service.

3) All types of cloud service usage shall be approved by the relevant department-level executive and the Digital Technology Department executive, with careful consideration of operational necessity and associated risks, including requests to store or process critical data on public cloud services.
4) The organization shall maintain and document a comprehensive Cloud Asset Inventory covering all assets residing in cloud environments, such as virtual machines, databases, storage, and other services, to enable appropriate control, auditing, and risk assessment. The inventory shall be reviewed and updated on a regular basis.

1.5.2. Data Security & Protection

1) Critical data and personal data stored or processed in cloud services shall be encrypted both at rest and in transit, to prevent unauthorized access or disclosure.
2) Prior to uploading data to cloud systems, the organization shall perform Information Classification to clearly define the sensitivity level of data, enabling appropriate controls to be applied in accordance with the risk level of each data type.
3) Data that is no longer required shall be managed in accordance with the Data Retention Policy or Data Deletion Policy, and shall be securely deleted or destroyed in accordance with the organization's defined standards, to prevent misuse or data leakage.

1.5.3. Secure Configuration & Hardening

1) The organization's cloud services shall be configured in accordance with widely accepted security practices, such as CIS Benchmarks or vendor best practices, to mitigate risks arising from misconfiguration.
2) Systems and services operating in cloud environments shall have clock synchronization configured in alignment with the organization's defined time standards, such as a centralized NTP server, to ensure that event logging, log analysis, and security event investigations can be conducted accurately and reliably.
3) Cloud systems shall be subject to robust network security controls, such as firewall rules to restrict access and reduce the risk of external and internal attacks. Necessary security tools and services, such as anti-malware and vulnerability scanning, shall be enabled to help prevent, detect, and mitigate security risks in the organization's cloud environment.

4) The organization shall continuously monitor, review, and evaluate the performance efficiency of cloud-based systems, including resource utilization, availability, and system capacity such as CPU, memory, network, storage, and other related services.

1.5.4. Backup & Business Continuity

1) Systems operating in cloud environments shall have data backups performed according to the criticality levels defined by the organization. Backups shall be conducted on a regular basis and stored securely.
2) The organization shall conduct regular backup restoration tests to ensure that data can be recovered accurately and in a timely manner when required.
3) Cloud services shall be incorporated into the organization's Business Continuity Plan and Disaster Recovery Plan (BCP/DRP), or shall be aligned with the capabilities and plans of the cloud service provider, to prevent operational impact in the event of a disruption.

1.5.5. Monitoring & Logging

1) Logs of significant security events shall be recorded, maintained for integrity, and retained in accordance with the organization's requirements. Log data shall be available for retrospective review and analysis.
2) The organization shall conduct regular log reviews to identify anomalous behavior or indicators of potential security incidents.

1.5.6. Privacy & Legal Compliance

1) The processing of personal data on cloud services shall comply with applicable laws and regulations, including the Personal Data Protection Act (PDPA) and any other relevant legislation governing the jurisdiction in which the data is stored or processed.

1.5.7. Incident Management

1) Cloud services shall be integrated into the organization's Incident Response Plan to enable systematic management of security incidents.
2) Cloud service providers shall notify the organization of security incidents within the timeframes and under the conditions specified in the SLA, to enable timely remediation and mitigation of damage.
3) The organization shall maintain clearly defined emergency contact channels and escalation procedures to support coordination with service providers or relevant internal units as required.

1.5.8. Termination & Exit Process

1) Upon termination of a cloud service, the organization shall carry out a secure decommissioning process, including deletion of user accounts, revocation of access rights, and complete management of all cloud resources.
2) The responsible party shall coordinate with the cloud service provider to ensure that all organizational data is securely deleted, and shall obtain a Data Deletion Certificate to confirm that the deletion has been carried out completely and in accordance with the organization's requirements.
3) The organization shall develop a Data Migration and Exit Plan to prevent vendor lock-in and to ensure that data can be securely and continuously migrated back or transferred to a new service provider.

Part 1.6 Budgeting and Accounting for Services Policy

Objective

To establish guidelines for managing budgets and controlling expenditures related to the support of information technology services in an appropriate and effective manner.

1.6.1. The Digital Technology Department shall ensure that budget allocations are complete and sufficient to support service delivery, and shall control expenditures to achieve maximum efficiency.

1.6.2. The Digital Technology Department shall ensure that budget allocations take into account all relevant cost components, including direct costs, indirect costs, IT asset procurement costs, shared resource costs, general and administrative expenses, externally supplied service costs, personnel costs, license expenses, and any other related costs associated with service delivery.

1.6.3. The Digital Technology Department shall monitor budget utilization and review remaining budget balances to ensure effective budget management.

Part 1.7 Service Level Management Policy

Objective

To establish guidelines for defining service level agreements for information technology services between the Digital Technology Department and the organization's information system users, at mutually acceptable levels.

1.7.1. The organization shall require the establishment of contracts specifying service level agreements as follows:

1) Service Level Agreement (SLA) between the service provider unit and users.
2) Operational Level Agreement (OLA) between internal service provider units within the organization.
3) Underpinning Contracts (UC) between the service provider unit and external parties.

1.7.2. The Digital Technology Department shall establish service agreements between the Digital Technology Department and users. Such agreements shall be formally approved by the Digital Technology Department executive and by management representatives from the relevant units within the organization.

1.7.3. The Digital Technology Department shall manage information technology service delivery in accordance with the established service agreements.

1.7.4. The Digital Technology Department shall periodically review and analyze service performance and trends as appropriate, and shall implement improvements to enhance operational efficiency on an ongoing basis.

1.7.5. Any amendments to documents relating to service requirements, service level agreements, or service catalogues shall be processed through the Change Management process as defined by the organization.

Part 1.8 IT Insourcing and IT Outsourcing

Objective

To establish requirements and an operational framework for the provision and use of information technology services within the organization, ensuring efficiency, security, and maximum benefit to the organization.

1.8.1. IT Insourcing

1) The Digital Technology Department shall establish controls and governance over information technology operations in accordance with all requirements relevant to the organization's business operations. The Digital Technology Department shall provide information technology services exclusively to internal units and subsidiaries of the organization.
2) The Digital Technology Department shall establish internal controls and develop Operation Procedure Manuals with a clear Segregation of Duties structure, and shall maintain regular records of operational activities.
3) The Digital Technology Department shall establish contingency measures, including emergency response plans and data backup arrangements, with backup cycles agreed upon with service recipients.

4) The Digital Technology Department shall ensure that data backups are performed using storage media and stored at locations specifically provided and prepared by the service recipient, or at mutually agreed locations. Service data belonging to the service recipient shall not be disclosed or used with any external parties.
5) The organization shall require service providers to manage service levels in accordance with the Service Level Management Policy as defined in part 1.7.

1.8.2. IT Outsourcing

The engagement of external service providers for information technology services shall be aligned with the organization's business strategy, with due consideration for the continuity, accuracy, and reliability of customer services. The following baseline criteria shall apply:

1) The criteria for engaging external service providers shall not conflict with any regulations or requirements issued by government authorities.
2) Business Continuity Management shall be established to ensure that the organization's and its subsidiaries' information systems are capable of continuing business operations and delivering customer services without interruption.
3) Guidelines for evaluating and selecting service providers shall be established to assess service reliability and to ensure that providers are capable of delivering services in accordance with the agreed service levels. External service providers shall also be required to complete a self-assessment using the IT and Cybersecurity Risk Assessment Form (F-DT-01-04).
4) Guidelines for maintaining information security and confidentiality shall be established to ensure that customer responsibilities are properly fulfilled and that appropriate customer protection measures are in place.
5) The performance of external service providers shall be regularly monitored, evaluated, and reviewed to ensure compliance with defined objectives and targets.
6) Risk management guidelines for the use of external service providers shall be established in writing, covering operational risk, strategic risk, reputational risk, and legal risk. Such guidelines shall be proportionate to the criticality of the systems supported by external parties, aligned with the overall risk management policy, and communicated to all relevant parties for acknowledgment and compliance.
7) External service providers shall be informed of and shall sign an acknowledgment of the organization's Code of Business Conduct.

Part 1.9 Information Security Incident Management

Objective

To establish guidelines for managing information security incidents, learning from errors and problems that arise, and implementing corrective improvements to prevent recurrence of information security incidents.

1.9.1. Management of Information Security Incidents and Improvements

1) Responsibilities and Procedures
   - The Digital Technology Department shall define responsibilities for managing unexpected or undesirable information security situations and shall clearly assign operational authority to personnel within the department.
   - The Digital Technology Department shall establish a process for distinguishing unexpected or undesirable information security situations from general operational incidents, in order to determine appropriate and effective remediation approaches.
   - The Digital Technology Department shall define reporting channels and criteria for reporting security-related events, weaknesses, or incidents, and shall communicate these to all organizational personnel and external parties for their awareness.
2) Assessment of and Decision on Information Security Events
   - System administrators shall assess information security-related events, classify and prioritize security events or weaknesses according to defined criteria, and notify relevant parties for remediation in cases where an event or weakness is identified as potentially having an information security impact.
3) Response to Information Security Incidents
   - Personnel designated to resolve information security incidents, as well as external parties engaged under contract, shall carry out incident resolution in accordance with the established information security incident response procedures.
   - Personnel designated to resolve information security incidents, as well as external parties engaged under contract, shall respond to and resolve information security incidents within the defined timeframes. In the event that resolution cannot be achieved within the specified timeframe, the matter shall be escalated to supervisors as promptly as possible.

4) Learning from Information Security Incidents)
    - Personnel designated to resolve information security incidents, as well as external parties engaged under contract, shall prepare analysis and resolution reports covering incidents, weaknesses, or vulnerabilities related to information security, and shall retain these as a knowledge base to support organizational learning and reduce the likelihood of recurrence.
5) Collection of Evidence)
    - Personnel designated to resolve information security incidents, as well as external parties engaged under contract, shall collect and preserve all evidence related to the information security incidents that have occurred, ensuring that sufficient evidence is gathered for presentation to relevant management and for use in any subsequent legal proceedings.

Part 1.10 Incident and Service Request Management Policy

Objective

To establish guidelines for resolving incidents, procuring, and managing the organization's computer systems in a manner that supports business service delivery with speed, continuity, accuracy, reliability, and efficiency.

1.10.1. Incident Management

1) The Digital Technology Department shall define criteria for measuring the Impact, Urgency, and Priority of incidents.
2) The Digital Technology Department shall define responsibilities for incident resolution and shall establish operational procedures for incident management and service request management to serve as operational guidelines.
3) The Digital Technology Department shall ensure that full details of incidents and service requests are recorded in accordance with the specified operational procedures, to serve as evidence and to support analysis, resolution, and performance reporting.
4) Digital Technology Department personnel shall resolve incidents and service requests received as promptly and effectively as possible, in accordance with the defined service level agreements.

1.10.2. In cases where the assigned handler is unable to independently resolve an incident or service request, the matter shall be escalated to relevant parties in accordance with the defined escalation sequence, to improve operational efficiency and response speed.

1.10.3. Service Request Management

1) Units requiring the procurement of computer systems shall specify their requirements, formulate a project proposal, and request budget approval in writing, with authorization from the department-level executive and the Information Technology Committee.
2) The Digital Technology Department shall provide relevant supporting information for computer system procurement, such as details of external service providers, hardware specifications, information security considerations, or any other information technology-related data as requested.

Part 1.11 Information Security Aspects of Business Continuity Management

Objective

To prevent disruption or interruption to the organization's business operations and to protect critical business processes from failures of information systems, and to ensure that information systems can be recovered within an appropriate timeframe.

1.11.1. Information Security Continuity

1) Planning Information Security Continuity
    - Data owners and the Digital Technology Department shall jointly identify events that may impact business processes and assess the risks associated with critical events and systems, in order to obtain accurate and complete information for use in developing an information security continuity plan.
2) Implementing Information Security Continuity
    - The Digital Technology Department shall develop a Disaster Recovery Plan that incorporates information security measures as an integral component, and shall ensure that the plan is aligned with the organization's Business Continuity Plan.
3) Verify, Review and Evaluate Information Security Continuity
    - The Digital Technology Department shall test the Disaster Recovery Plan at least once a year and shall document the test results, to ensure that the plan is accurate and capable of effectively supporting operational recovery.
    - Personnel involved in information system recovery operations shall possess the necessary technical knowledge for system recovery and shall participate in plan rehearsals.

- Data owners and system users associated with the Business Continuity Plan shall participate in plan testing and carry out activities in accordance with the defined plan.

1.11.2. Redundancies

1) Availability of Information Processing Facilities

- The organization shall ensure that availability requirements for critical information systems are assessed and documented.
- The organization shall ensure that adequate backup information systems, redundant equipment, or supporting infrastructure are installed to maintain appropriate business continuity.

Part 1.12 Business Continuity Management

Objective

To establish guidelines for managing the continuity of information system services in the event of any emergency or information security incident that may cause disruption to the organization's business operations.

1.12.1. The organization shall ensure that data backup and information system recovery capabilities are in place to maintain continuous business processes and minimize the impact of any event causing business disruption. The most senior executive of the organization shall serve as the ultimate decision-making authority in such situations.

1.12.2. Service recipient units and the Digital Technology Department shall jointly establish a framework to support business continuity, covering the defined information security requirements and facilitating the prioritization of plans and activities to be executed.

1.12.3. Service recipient units and the Digital Technology Department shall conduct risk assessments, document risks that may cause disruption to information system services, and establish written agreements on recovery requirements, including the Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

1.12.4. Service recipient units and the Digital Technology Department shall ensure that Business Continuity Plans are developed within the defined framework and disseminated to all relevant parties. Business Continuity Plans shall be tested at least once a year.

1.12.5. The Digital Technology Department shall develop a Disaster Recovery Plan (DRP) in alignment with the organization's Business Continuity Plan.

1.12.6. The Digital Technology Department shall ensure that data, documents, software, systems, equipment, and necessary personnel are backed up and maintained to support the fastest possible recovery of information systems following a service disruption or disaster.

1.12.7. The Digital Technology Department shall conduct Disaster Recovery Plan (DRP) tests at least once a year and shall document the test results, to ensure that business operations can continue when events affecting the organization's business processes occur.

Part 1.13 Compliance

Objective

To ensure that the organization's operations comply with applicable laws, agreements, contracts, and security requirements that the organization and its personnel are obligated to observe, and to ensure that compliance with the defined information security policies is regularly reviewed.

1.13.1. Compliance with Legal and Contractual Requirements

1) Identification of Applicable Legislation and Contractual Requirements
   - The Digital Technology Department shall collaborate with the Legal Department and the Human Resources Department to compile applicable laws, regulations, criteria, and requirements related to information security, and shall document these as written operational requirements, kept up to date on a regular basis.
   - All personnel shall be strictly responsible for complying with the identified requirements.
   - Personnel shall not use the organization's information technology assets and systems to carry out any action that conflicts with the laws of the Kingdom of Thailand or international law under any circumstances.

2) Intellectual Property Rights
   - The Digital Technology Department shall establish processes for managing the use of licensed software and intellectual property, to ensure that the use of information that may constitute intellectual property, or the use of commercially developed software, is compliant with applicable laws and contractual requirements.

- Users shall not copy or distribute software for which the organization has purchased a license, except for the purpose of creating an emergency backup or a replacement copy of the original software.
- Users are strictly prohibited from reproducing or distributing images, articles, books, or any documents in a manner that infringes copyright, or from installing unlicensed software on the organization's information systems.
- Software developed for the organization, whether by external parties or by internal personnel, is considered organizational property. The organization does not permit external parties or internal personnel to copy or distribute such software without authorization.
- Users of software on the organization's information systems shall strictly adhere to copyright law, the information security policy, and the requirements of the software manufacturer.
- Employees are prohibited from playing unlicensed music or music not provided by the Company through the Company's broadcasting system, including music played from legitimately licensed recordings or from public networks such as radio or YouTube, as such actions constitute copyright infringement under the Copyright Act B.E. 2537 with respect to the unauthorized public communication of copyrighted works.

3) Protection of Records
   - Data owners shall comply with legal obligations relating to specific categories of information, such as accounting and customer data, and shall establish data management requirements and retention periods in accordance with such obligations.
   - Data owners shall control and prevent event logs from being damaged, lost, altered, accessed, or disclosed without authorization, in a manner consistent with applicable laws, regulations, and business requirements.
4) Privacy and Protection of Personal Identifiable Information
   - The organization shall ensure that personal data is protected in compliance with applicable laws, government-issued regulations and criteria, and all other binding requirements applicable to the organization.

- Customer information is considered sensitive. The unit responsible for managing such data shall ensure that only personnel and employees assigned in accordance with their job responsibilities, or those authorized by their supervisors, may modify such information.
- Personal information of personnel, employees, and customers is considered confidential and may only be disclosed to authorized individuals as defined by the organization.

5) Regulation of Cryptographic Controls
   - The Digital Technology Department shall ensure that cryptographic controls are implemented in compliance with applicable laws, government-issued regulations and criteria, and all other binding requirements applicable to the organization.

1.13.2. Information Security Reviews

1) Independent Review of Information Security
   - The organization shall arrange for information security assessments to be conducted by an internal audit unit or an independent external auditor, to verify compliance with information security policies, standards, and procedures, and to review the adequacy of information system controls and adherence to those controls.

2) Compliance with Security Policies and Standards
   - Supervisors of each department shall be responsible for regularly reviewing the compliance of their subordinate personnel with relevant information security policies, standards, and procedures.
   - In cases where a department supervisor identifies non-compliance with policies, standards, or procedures that has not yet impacted the organization's information security, the supervisor shall advise and ensure that the subordinate personnel understand the requirements. However, where the identified non-compliance has an impact on the organization's information security, the supervisor shall take disciplinary action in accordance with the organization's regulations.
   - The Digital Technology Department shall provide advisory support on the use of, or compliance with, information security policies, standards, procedures, and related requirements to other units upon request.

3) Technical Compliance Review
   - Technical reviews of information systems shall be conducted on a regular basis, including penetration testing, to ensure compliance with the information security policy and international information security standards.
   - The system audit unit shall review the technical controls of information systems to verify that they are adequate, appropriate, and being adhered to.
   - System administrators shall conduct regular assessments of information system security standards, such as Vulnerability Assessments and Penetration Tests, to ensure compliance with the information security policy and international information security standards.

Part 1.14 Documented operating procedures

Objective

To establish principles and standards for the creation, storage, and dissemination of operational procedures related to data processing, in order to ensure that operations are accurate, secure, and compliant with defined standards.

1.14.1. The Digital Technology Department shall establish written operational procedures for critical information systems, with a clear segregation of personnel responsibilities in accordance with a defined operational structure, to enable personnel to perform their duties correctly and in compliance with the organization's Information Technology and Information Security Policy. Such procedures shall be established in the following circumstances:
   - When an activity is required to be performed in the same manner by multiple individuals.
   - When an activity is performed infrequently.
   - When an activity is new and carries risk if performed incorrectly.
   - When an activity is to be handed over to a new employee, another individual, or another unit.

1.14.2. Documentation of operational procedures for organizational activities related to information security shall specify the responsible party, installation methods or secure system configuration settings, both automated and manual information processing and handling procedures, security measures, guidelines, applicable conditions, and contact channels for both internal and external support, among other relevant details.

1.14.3. Units within the Digital Technology Department shall develop manuals, system documentation, and knowledge bases to ensure that relevant parties have a clear understanding of systems, job characteristics, and work processes.

1.14.4. Units within the Digital Technology Department shall keep operational practices, manuals, system documentation, and knowledge bases up to date at all times, and shall ensure that such procedures are in a ready and accessible state. Relevant parties shall be informed and required to comply accordingly.

1.14.5. The Digital Technology Department shall control and govern change management for changes to organizational structure, operational procedures, and information systems, to ensure that controls are in place prior to any changes, modifications, or actions that may affect the operation of any system. Such activities shall be carried out in accordance with the Change Management Policy.

Section 2: Human Resource Security Policy

Part 2.1 Human Resources Security

Objective

To establish measures for controlling, governing, and monitoring the recruitment of personnel into the organization, the management of personnel during employment, and the management of personnel upon separation from employment or change of job responsibilities.

2.1.1. Prior to Employment

1) Screening
   - The organization shall require background checks to be conducted on job applicants and external parties who are required to provide services within the organization.

2) Terms and Conditions of Employment
   - The Human Resources Department shall ensure that employment contracts or work agreements for personnel, as well as contracts with external organizations or individuals, are signed. Such contracts shall specify information security responsibilities, and users shall acknowledge and accept the organization's regulations by reading, understanding, and complying with the policies and rules established by the organization.

3) Employment contracts, work agreements for personnel, and contracts with external organizations or individuals shall specify information security responsibilities and include a Non-Disclosure Agreement (NDA), in alignment with the information security policy and defined operational procedures.

2.1.2. Confidentiality or Non-Disclosure Agreements

1) Department-level executives shall ensure that personnel and external parties performing work for the organization sign written confidentiality or non-disclosure agreements, including the Supalai Partner Code of Conduct.

2.1.3. Confidentiality agreements shall extend to the preservation of confidentiality after the termination of the contract and shall be established in documentation.

2.1.4. During employment

1) Management Responsibilities
    - Department-level executives shall establish controls and ensure that personnel, or external parties engaged to perform work or provide services to the organization, comply with the Information Technology Policy and the information security procedures announced by the organization.
2) Information Security Awareness, Education and Training
    - The Digital Technology Department shall provide channels through which personnel can study and understand the information security policy, as well as their own information security roles and responsibilities, before being authorized to commence work with the organization.
    - The Digital Technology Department shall arrange training on general operational topics by the responsible unit on a regular basis, to enable engaged personnel to learn and understand relevant subjects, such as system usage, commercial software usage, basic computer troubleshooting, and compliance with applicable laws, regulations, and requirements.
    - The Digital Technology Department shall conduct security awareness training on a regular basis to enable engaged personnel to learn and understand relevant topics, and to support them in performing their responsibilities effectively and securely.
3) All units of the Company shall ensure that personnel and external service providers strictly comply with the defined regulations.

4) Disciplinary Process)

- The organization shall establish a disciplinary process to address users who violate or breach the Information Technology Policy, information security procedures, or any operational procedures related to the organization's information security.

2.1.5. Termination or Change of Employment

1) Termination or Change of Employment Responsibilities

- The Human Resources Department shall establish written regulations and responsibilities relating to information security for personnel and external parties following separation from employment or a change in employment responsibilities.

Part 2.2 Remote working

Objective

To ensure that working from outside the organization or the use of mobile devices is carried out with adequate security.

2.2.1. Teleworking

1) All users working from outside the office shall comply with the organization's information security policy in the same manner as when working within the office.
2) Users who access organizational information for work outside the office or via remote access shall obtain authorization from the information asset owner and their direct supervisory unit, with justifiable reasons.
3) Users requiring remote access shall obtain authorization from the system administrator prior to accessing the system.

Part 2.3 Reporting Information Security Events

Objective

To support the timely, consistent, and effective reporting of information security events.

2.3.1. Reporting Information Security Events

1) Users and external parties shall report information security-related events to their supervisors and the Digital Technology Department through the defined reporting channels as promptly as possible.

2.3.2. Reporting Information Security Weaknesses

1) Users and external parties shall report information security weaknesses to their supervisors and the Digital Technology Department through the defined reporting channels as promptly as possible.
2) Users and external parties who discover an information security breach or any weakness in the organization's information systems shall not disclose the incident to others, except to their supervisors and the Digital Technology Department, and shall not attempt to independently investigate or test the suspected security weakness.

Section 3 Physical Security Controls Policy

Part 3.1 Physical and Environment Security

Objective

To establish measures for protecting, controlling the use of, and maintaining the physical condition of information assets and equipment that form the infrastructure supporting the organization's information systems, ensuring they remain in a complete and ready state, and to prevent unauthorized access to information assets or unauthorized disclosure of information.

3.1.1. Secure Area

1) Physical Security Perimeter
    - The organization shall assess and establish secure areas comprising physical barriers, walls or perimeter fencing, main entry and exit points, and appropriate security systems.
2) Physical Entry Controls
    - The organization shall restrict access to operational areas and areas containing critical information to authorized personnel only.
    - The list of personnel authorized to access operational areas and areas containing critical information shall be regularly reviewed, updated, and maintained.
    - The Digital Technology Department shall establish access controls for secure areas, including computer rooms and system administrator work areas, restricting entry and exit to authorized personnel only. Access records for computer rooms shall be maintained, capturing details of individuals, entry and exit times, and purposes of access, and such records shall be reviewed on a regular basis.

3) Securing Offices, Rooms, and Facilities
    - The Digital Technology Department shall design and implement physical security systems to protect operational areas, areas containing critical information, computer rooms, system administrator work areas, and information equipment from damage and unauthorized access.
4) Physical security monitoring
    - Surveillance of premises, building access points, and areas housing critical systems shall be conducted through alarm systems, monitoring systems, or security personnel.
    - Surveillance systems such as CCTV shall be installed to record entry and exit activity both inside and outside the premises.
    - Detection and monitoring equipment shall be regularly tested to ensure operational readiness and the ability to trigger alerts upon intrusion.
5) Protecting Against External end Environmental Threats
    - The Digital Technology Department shall ensure that physical security measures are designed and implemented to protect against external threats, whether caused by human actions or natural events, such as fire, flooding, earthquakes, explosions, and civil disturbances.
6) Working in Secure Areas
    - The Digital Technology Department shall establish and enforce physical security guidelines for working in secure areas, including computer rooms and system administrator work areas, and shall ensure strict adherence to such guidelines.
7) Delivery and Loading Areas
    - The Digital Technology Department shall establish controls over areas where unauthorized individuals may potentially gain access, by designating separate areas for goods delivery and for the preparation or assembly of information equipment prior to introduction into computer rooms, to prevent unauthorized access to information systems and data.

3.1.2. Equipment

1) Equipment Setting and Protection
    - The Digital Technology Department shall place information equipment in secure rooms or areas. Cabinet doors housing servers and network communication equipment shall remain locked at all times, with only authorized personnel permitted to open them for maintenance or reconfiguration purposes, to reduce the risk of unauthorized access.
2) Supporting Utilities
    - The Digital Technology Department shall ensure that failure prevention and supporting utility equipment is installed within computer rooms, including fire suppression systems, smoke detectors, uninterruptible power supplies, temperature and humidity control systems, water leak detection systems, and information equipment fault alert systems. All such equipment shall be maintained in a ready and operational state at all times.
3) Cabling Security
    - The Digital Technology Department shall ensure that the installation and maintenance of power cables and communication cabling in operational areas and computer rooms comply with industry safety standards, to prevent unauthorized access, data interception, or physical damage.
4) Equipment Maintenance
    - The Digital Technology Department shall ensure that all primary information system equipment used in operational processing, as well as supporting utility equipment, is maintained at the intervals and in accordance with the requirements recommended by manufacturers, to ensure continuous operation and maintained readiness.
    - The Digital Technology Department shall ensure that equipment maintenance activities are recorded, along with any identified faults or deficiencies, to support ongoing assessment and improvement of equipment readiness.
5) Removal of Assets
    - Personnel responsible for managing secure areas and premises shall not permit information equipment to be removed from the organization unless authorized by a designated asset removal authority.

- Users shall not remove information equipment, data, or software from the organization without authorization from the designated asset removal authority.
- The Digital Technology Department shall establish written procedures for the removal of assets from the premises, keep them up to date, and communicate them to internal users for acknowledgment and compliance.

6) Security of Equipment and Asset Off - Permission
   - Department-level executives and above shall serve as the authorizing authority for the use of organizational information equipment off-premises, and shall ensure that appropriate protective measures are in place for equipment used outside the organization, taking into account the associated risks.
   - The Digital Technology Department shall establish security measures to control assets used off-premises, to mitigate risks arising from the removal of organizational equipment or assets.
7) Unattended User Equipment
   - The Digital Technology Department shall establish controls to protect unattended computers and information equipment from unauthorized access.
   - System administrators shall require users to protect their computers and information technology systems from unauthorized access by requiring correct password entry before use.
   - Users shall log out of information systems, computer systems, or computers immediately when they are no longer required or upon completion of work.
   - Users shall lock the screens of computers or critical devices when not in use or when leaving their workstations.
8) Clear Desk and Clear Screen Policy
   - System administrators shall ensure that computer screens are automatically locked after a period of inactivity not exceeding 15 minutes, and that session timeout settings are configured to prevent unauthorized access to data or systems.
   - Users shall not leave critical information, such as paper documents or storage media, in unsecured locations, public areas, or places where they may be easily observed. Users shall store information in appropriate locations with adequate access controls to prevent unauthorized access.

- Users shall not store critical data on the computer desktop. Users shall organize data storage on their computers and implement appropriate access controls to prevent unauthorized access to critical information.

3.1.3. Media Handling

1) Management of Removable Media
   - The Digital Technology Department shall establish written procedures for managing removable data storage media, keep them up to date, and communicate them to internal users for acknowledgment and compliance.
   - The management of removable media shall be consistent with the organization's defined information classification levels.
2) Disposal of Media
   - The Digital Technology Department shall establish media disposal procedures to prevent the leakage of confidential or sensitive information.
   - The Digital Technology Department shall define controls for media disposal in accordance with internationally accepted standards.
3) Physical Media Transfer
   - The Digital Technology Department shall establish operational procedures or information security requirements governing the transfer of storage media outside of its installation or operational area.

3.1.4. Secure Disposal or Re-Use of Equipment

1) Equipment containing storage media shall be inspected to ensure that critical information or licensed software stored on the media has been appropriately deleted, transferred, or destroyed in accordance with the applicable information classification level, prior to the disposal, sale, or reuse of the equipment.

Section 4: Technological Controls Policy

Part 4.1 User Endpoint Device Security Policy

Objective

To protect information from risks arising from the use of all types of user endpoint devices used to access organizational systems, such as desktop computers, laptops, notebooks, mobile devices, tablets, work mobile phones, storage accessories such as external drives, USB drives, and portable storage, as well as personally owned devices authorized for work use (BYOD), including devices belonging to personnel, contractors, and external parties authorized to connect to the organization's network or systems.

4.1.1. User Endpoint Device Security

1) Device Authorization and Registration
   - All devices used to access the organization's data or systems must be approved by the Digital Technology Department prior to use.
   - Devices must be registered in the Asset Inventory with key details recorded, such as owner, device serial number, operating system, and security status.
2) Secure Configuration
   - All devices must be configured in accordance with the organization's security standards, such as disabling unnecessary services, setting strong passwords, enabling firewalls, and applying appropriate operating system security settings.
   - Users are strictly prohibited from modifying, disabling security controls, or installing any software not approved by the organization.
3) Access Control
   - Devices must be configured with strong passwords or authentication mechanisms and set to lock automatically after a defined period of inactivity.
   - Access to critical systems must use Multi-Factor Authentication (MFA). Users are prohibited from sharing accounts or passwords with others under any circumstances.
4) Data Protection
   - All devices storing organizational data should have full-disk encryption enabled to prevent unauthorized access.

- Critical data must be stored in approved systems such as the organization's cloud or file servers. Storing critical data on personal devices or unauthorized locations is prohibited.

5) Software and Security Updates
   - Devices must have only software and applications approved by the Digital Technology Department installed.
   - Operating systems, antivirus programs, and security patches must be regularly updated according to defined schedules. Devices must have malware detection and prevention systems enabled at all times to protect against potential threats.

6) Network Security
   - Devices must connect to the organization's network through secure channels such as the organization's designated VPN. Connecting to unencrypted or high-risk public Wi-Fi networks that may be susceptible to data interception is prohibited.
   - Devices must undergo security verification before being permitted to access the organization's systems (Network Access Control).

7) Protection Against Lost or Stolen Devices
   - Users must maintain proper custody of devices and must not leave them unattended in unsecured locations. In the event that a device is lost or stolen, the user must immediately notify their supervisor and the Digital Technology Department so that risk control measures can be taken, such as suspending user accounts or initiating a remote data wipe.

4.1.2. Mobile Computing and Teleworking

1) Mobile Computing and Communication
   - The Digital Technology Department shall establish appropriate measures to ensure the security of mobile devices, taking into account the risks associated with connecting such devices to the organization's computer network and with using them off-premises.
   - All users who use mobile devices to connect to the organization's information systems must strictly comply with the information security policy and maintain a strong awareness of information security.
   - Users must take care to prevent others from viewing information on their screens in public places (Screen Privacy).

4.1.3. Bring Your Own Device : BYOD

1) Personnel are not permitted to use personal mobile devices or portable computers for organizational work without authorization.
2) Personal devices authorized for work use must comply with the same security measures as organizational devices.
3) The organization reserves the right to install security control systems such as Mobile Device Management (MDM) and to wipe organizational data from personal devices if security requirements necessitate it. Users must sign a consent agreement acknowledging the BYOD terms and conditions prior to use.

Part 4.2 Access Right Management Policy

Objective

To establish guidelines for managing access rights to the organization's data, information systems, and resources, ensuring that users are granted appropriate rights in accordance with their responsibilities, and preventing unauthorized access. This covers both internal and external users who have been granted access to the organization's data, resources, or information systems.

4.2.1. Privileged access rights

1) Privileged Account Management
    - The Digital Technology Department is responsible for defining processes for managing and controlling privileged access rights, to prevent data breaches and unauthorized access, and for administering, modifying, or revoking access to systems or information equipment with privileged access rights only as operationally necessary.
    - The Digital Technology Department shall establish written procedures for managing privileged user accounts, and communicate these to relevant parties for acknowledgment and compliance.
    - Access rights must be granted based on the principles of Least Privilege and Need-to-Use only. Permanent elevated privileges shall not be granted unless strictly necessary. Just-in-Time Access (JIT) or temporary privilege assignment for specific tasks should be used where applicable.
    - Authentication must be required for system access to ensure security, and usage must be monitored within the defined access timeframe.

- Privileged accounts must be clearly created, categorized, and controlled. Standard user accounts and administrator accounts must be kept separate.
- Privileged accounts must not be used for general tasks such as internet browsing, reading email, or routine work.
- Service accounts, API accounts, and automation accounts must be controlled, audited, and have their passwords securely stored.

2) Authentication & Protection
   - Privileged accounts must use Multi-Factor Authentication (MFA), and passwords must be complex and comply with the organization's Password Policy.
   - Passwords must be rotated regularly, or changed immediately upon identification of a security risk.
   - For high-risk operations, a Privileged Access Management (PAM) system should be used to control and log usage.
3) Usage Control
   - The use of privileged access must be limited to necessary cases with clear justification. Actions on critical operations such as changing system configurations, deleting data, adding users, or modifying permissions must be logged and retained as evidence.
   - Access for emergency troubleshooting must be accompanied by a record of the reason and duration of use.
   - Once a user no longer requires privileged access, all such rights must be revoked immediately.
4) Management of Privileged Access Right
   - The Digital Technology Department shall securely store privileged account credentials, such as administrator or root accounts on servers or application administrator accounts, and shall allow their use only when operationally necessary.
   - Passwords for privileged accounts must be changed at least every 90 days, and Multi-Factor Authentication (MFA) must be enabled where the system supports it. The password rotation period may be adjusted in accordance with the risk level and appropriateness of each system.
   - The organization may require immediate password changes upon identification of any security risk, whether technical, operational, or any event that may lead to unauthorized access to systems or data, in order to prevent and mitigate potential impact.

4.2.2. Management of Secret Authentication Information of Users

1) The Digital Technology Department shall establish written procedures for managing users' secret authentication information, keep them up to date, and communicate them to internal users for acknowledgment and compliance.

4.2.3. Information access restriction

1) Application and Information Access Control
    - The data owner and system administrator shall define and establish appropriate usage procedures for critical information systems, including data, computer systems, applications, electronic mail (e-mail), wireless networks (Wireless LAN), and internet services. Access rights shall be granted strictly based on job responsibilities and must be formally approved in writing and properly documented by the authorized supervisor of the respective department.
2) Secure Log-on Procedures
    - The Digital Technology Department shall establish written secure log-on procedures for information systems based on internationally accepted standards, keep them up to date, and communicate them to internal users for acknowledgment and compliance.
3) Use of Privileged Utility Programs
    - The Digital Technology Department shall control the use of utility programs and restrict access to utility programs for critical information systems or computer programs, to prevent the circumvention of established security measures, as certain utility programs may enable users to bypass system security controls.
4) Restrictions on Changes to Software Packages
    - Commercial software packages used within the organization should be used without modification. Where changes to a software package are unavoidable, the unit assigned to carry out the changes must apply strict change control measures.
    - Any modifications to commercial software packages must be carried out in accordance with the change control procedures defined by the Digital Technology Department.

5) Access to source code
   - The Digital Technology Department shall establish controls over access to program source code and the use of source code in development activities, to prevent errors in the development of information systems and organizational applications.

Part 4.3 Operations Security

Objective

To establish controls ensuring that the organization's information security operations and communications management have clear, well-defined, and secure operational procedures.

4.3.1. Capacity Management

1) Capacity Management
   - System administrators shall assess the capacity and adequacy of information resources such as server and network device utilization, including CPU, memory, disk storage, and network bandwidth, and shall plan for future information resource requirements to ensure that information systems maintain appropriate and sufficient performance.
   - System administrators shall continuously monitor the performance of critical systems and information equipment to ensure continuous and efficient operation, and shall record resource utilization on an ongoing basis, including CPU, RAM, storage, network, database performance, and cloud resources.
   - Threshold alerts must be configured to notify administrators when resource utilization approaches critical levels, enabling timely remediation or capacity expansion.
   - The Digital Technology Department shall produce regular capacity and performance reports, and resource utilization data shall be analyzed to inform investment decisions and system planning.

4.3.2. Protection from Malware

1) Controls Against Malware
   - The Digital Technology Department shall establish measures for the detection, prevention, and recovery of systems to protect assets from malicious software, and shall provide appropriate security awareness to users.
   - All work computers must have antivirus or anti-malware software installed.

- All data, files, software, or other items received from other personnel must be scanned for computer viruses and malicious programs before use or storage.
- When a user discovers that a computer is infected with a virus, the user must immediately disconnect the computer from the network and notify the system administrator for immediate investigation and remediation.

4.3.3. Technical Vulnerability Management

1) Management of Technical Vulnerabilities
   - Designated personnel or system administrators are responsible for monitoring technical vulnerabilities and identifying preventive measures for implementation.
   - The Digital Technology Department shall ensure that the organization's information systems are assessed for potential technical vulnerabilities at least once a year.
   - System administrators shall maintain and service systems on a regular basis to sustain information security levels, including vulnerability scanning, risk assessment of identified vulnerabilities, and remediation of information system vulnerabilities.

4.3.4. Configuration management

1) Establishing and Reviewing Configuration Standards
   - The organization shall define and document baseline configurations for all critical hardware, software, networks, and services. The following considerations shall be taken into account when establishing and reviewing configuration standards:
     - Minimize the number of personnel with administrator privileges.
     - Disable accounts that are unnecessary, inactive, or lack adequate security maintenance.
     - Disable functions and services that are unnecessary, inactive, or lack adequate security maintenance.
     - Restrict the use of programs or parameters that may have a significant impact on systems, including the operating system.
     - Change vendor default or factory settings immediately upon installation, particularly those affecting security, such as default passwords.

- Changes to configuration data must be subject to version control and must be approved by the responsible party and relevant units through the Change Management process.
- Actual system configurations must be periodically verified against the defined baseline according to the organization's review cycle, and settings must be kept up to date.

4.3.5. Backup

1) Information Backup
   - The Digital Technology Department shall establish backup measures and define backup schedules for critical information systems on a regular basis to prevent data loss.
   - Data owners shall ensure that information is backed up regularly and kept current, and that backup data is tested on a regular basis to ensure that data can be successfully restored when required.
   - The Digital Technology Department shall be responsible for performing backups and storing media in separate locations to protect against cybersecurity threats, such as cloud storage, and shall ensure that backups are stored in appropriate locations with no risk of data leakage.
2) Redundancy of information processing facilities
   - The organization shall design and implement system resilience for information processing equipment in accordance with service criticality levels, such as backup power supplies, network redundancy, and redundant connection paths, to ensure continuous service availability and minimize the impact of failures.
   - The organization shall establish contracts or agreements with external service providers that incorporate security and service continuity measures, to ensure that systems and processing equipment remain available in accordance with organizational requirements.
   - The organization should consider establishing a Disaster Recovery Site or secondary cloud region, separate from the primary Data Center, to support operations in the event that the primary Data Center becomes unavailable.
   - Backup equipment must be maintained according to defined schedules, such as UPS battery inspections and generator tests, with results recorded.

4.3.6. Restrictions on Software Installation

1) Installation of software on operational systems
    - The Digital Technology Department shall establish procedures and controls for software installation on production systems, to restrict user-initiated software installation and prevent the installation of unauthorized software.
    - The Digital Technology Department shall maintain a written Standard Software List specifying software approved for installation on organizational computers, keep it up to date, and communicate it to internal users for acknowledgment and compliance.
    - Users shall comply with software installation control rules and shall not install unlicensed software on organizational computers.

4.3.7. Logging and Monitoring

1) Event Logging
    - System administrators shall retain event log data relating to information security in sufficient detail to support auditing requirements.
    - System administrators shall continuously monitor information system usage, and monitoring results must be reviewed regularly to detect anomalies.
    - System administrators shall ensure that fault logging is implemented for information system-related errors, and shall analyze, remediate, and establish preventive measures to avoid recurrence.
2) Protection of Log Information
    - System administrators shall ensure that log data and systems for recording and storing information system usage evidence are protected against unauthorized modification, damage, or access.
3) Administrator and Operator Logs
    - System administrators shall ensure that the operational activities of system administrators and relevant system operators are logged, including system start and shut-down times.
    - System configuration changes, system errors, and corrective actions. Activity logs must be reviewed on a regular basis.

4) Clock Synchronization

- System administrators shall ensure that the organization's information equipment and information systems have synchronized time settings referenced against an accurate and internationally recognized time source.
- System administrators shall regularly verify and update the time settings of information equipment and systems to prevent inaccurate timestamps from being recorded.

Part 4.4 Data Security Policy

Objective

To protect sensitive data from unauthorized access, loss, or leakage, while maintaining data availability and integrity. Information deletion ensures that sensitive data is permanently removed from systems when it is no longer required.

4.3.1. Data Security Policy

1) Information Deletion

- The organization shall define clear Data Retention Periods for each category of data, taking into account business necessity, legal requirements, and information security. Data that is no longer required must be managed through a secure deletion or destruction process in accordance with the organization's defined standards.
- Data that has exceeded its retention period must be deleted in accordance with the defined Data Retention Period and applicable legal requirements.
- Data deletion must employ secure methods such as Secure Erase, Cryptographic Erasure, or Overwriting in accordance with the organization's defined standards.
- Storage devices such as hard disks, SSDs, USB drives, and storage media that are to be decommissioned must have their data securely deleted prior to sale, disposal, or transfer.
- Data deletion in cloud systems must be confirmed by the service provider, such as through a Data Deletion Certificate.
- Evidence of data deletion must be recorded and retained for the defined period.

2) Data Masking
   - The organization shall apply data masking techniques to prevent the disclosure of critical or personal data, particularly in testing, development, or data sharing processes.
   - Sensitive data or personal data must be masked or de-identified when used in non-production environments such as test or development systems.
   - The organization should consider de-identification techniques such as tokenization, data masking, pseudonymization, or anonymization.
   - Access to masked data and source data must be controlled, with access granted only to those with a genuine need.
   - Data masking methods must be reviewed to ensure that data cannot be re-identified.
   - Sensitive data in its original form must not be used in environments that lack adequate protective measures.
3) Data Leakage Prevention
   - The organization shall establish data leakage surveillance measures across all data transmission channels to prevent unauthorized leakage or exfiltration of data, such as by implementing Data Loss Prevention (DLP) solutions to detect, prevent, and alert on abnormal data movement.
   - Data transmission channels must be defined and controlled, and technical measures must be implemented to restrict unauthorized data exfiltration from the organization, such as disabling USB ports on work devices, controlling email-based data transfers, restricting cloud storage usage, controlling file transfers, and limiting mobile device connectivity.
   - Confidential data transmitted outside the organization must be encrypted and authorized by an authorized person prior to transmission.
   - Personnel must receive training on behaviors that risk data leakage, such as sending data to the wrong recipient, sharing through insecure channels, or using unauthorized applications.
   - Data leakage incidents must be logged and investigated in accordance with the Incident Management Process.
   - Access to critical data must be governed by the principle of Least Privilege and subject to continuous Monitoring and Logging.

Part 4.5 Service Reporting Policy

Objective

To provide data services for the preparation of management reports, support organizational operations and competitiveness, and ensure that reports contain accurate and complete information that relevant parties can access and use correctly.

4.5.1. Provision and Maintenance of Data Sources and Management Reports

1) Internal units shall provide management with operational performance reports and information useful for business decision-making, enabling management to make informed decisions promptly and in a timely manner.
2) Internal units should classify data in data sources and management reports at the Highly Restricted level, and such data must not be disclosed to others without authorization.
3) The Digital Technology Department shall provide data sources to support each unit in utilizing data for analysis or research to enhance business competitiveness in a timely manner.
4) The Digital Technology Department shall maintain data sources, operational performance data, and all information used for management reports in a state of accuracy and readiness at all times.
5) The Digital Technology Department shall support the development of data literacy skills among users in each unit to enable them to produce reports accurately and efficiently.

4.5.2. Report Printing

1) When a user requires the printing of highly sensitive reports, the unauthorized disclosure of which may have a significant impact on the organization, the user must obtain approval from the executive of the data-owning department prior to each printing.
2) Users should maintain a register for tracking the printing, distribution, and storage of all printed reports in a secure manner.
3) Users should require a signature upon receipt of reports, and reports that are no longer in use should be destroyed.

4.5.3. Access to Data Sources

1) Users must request access rights to data sources from the data-owning unit prior to accessing any data source.

4.5.4. Data Quality Control

1) Users are responsible for data cleaning and must submit requests for data processing through the e-Memo system to the Digital Technology Department, so that IT staff can extract and update data in the system accordingly.
2) Where a user requires changes to data in a data source, the user must prepare the data in accordance with the data cleaning process and submit a change request through e-Memo to the Digital Technology Department, so that IT staff can update the data in the database accordingly.

Part 4.6 Communications Security

Objective

To establish controls for managing the organization's computer network and the transmission of data through both internal and external computer networks in a secure manner.

4.6.1. Network Security Management

1) Network Controls
    - System administrators shall control and govern the management of computer network controls to protect against threats, and to maintain the security of information systems and applications operating on the network, as well as information exchanged across the network.
    - System administrators shall maintain a Network Diagram with details of the internal and external network boundaries and connected devices, kept up to date at all times.
    - The use of the organization's internet for personal commercial purposes is prohibited, as is accessing inappropriate websites such as those containing immoral content, content that may affect or threaten national security, religion, or the monarchy, or websites that are harmful to society or that infringe upon the rights of others or may cause damage to the Company.
    - Employees or users on the organization's network are prohibited from acting in the name of the organization through social media or representing their actions as being conducted on behalf of the organization, unless they are employees or users who have been explicitly authorized to do so by the organization.

- Presenting or posting organizational information in an inappropriate manner or as personal opinions about the organization in social media networks in a way that may cause misunderstanding is to be avoided.

2) Security of Network Services
   - System administrators shall ensure that the security features, service levels, and management requirements for all network services, whether provided internally or externally, are specified in the applicable network service agreements or contracts.
3) Segregation in Network
   - The Digital Technology Department shall implement appropriate network segregation, taking into account user access requirements, information security implications, and the sensitivity level of data residing on each network segment.

4.6.2. Information Transfer

1) Information Transfer
   - The Digital Technology Department shall establish operational procedures for information transfers appropriate to the type of communication used and the information classification level of the data.
2) Agreements on Information Transfer
   - The Digital Technology Department shall ensure that agreements for information transfer are established for both internal exchanges and exchanges between the organization and external parties.
   - Transfers of information from the organization to external parties must be approved by the data owner prior to each transfer, governed by written agreements specifying the terms and conditions of the exchange, and protected in accordance with the applicable information classification level.
3) Electronic Messaging
   - The Digital Technology Department shall establish controls for electronic messaging such as email, Electronic Data Interchange (EDI), and instant messaging. Critical electronic messages must be adequately protected against unauthorized access attempts, modification, disruption, or denial of service.

4) Securing Application Service on Public Networks
   - Information security shall be maintained for data passing through application services, both in general use and when transmitted over public networks, to prevent fraudulent activities, incomplete or misdirected transmissions, and unauthorized disclosure, copying, or modification of data.

4.6.3. Web Filtering

1) The organization shall restrict website access or implement a web filtering system to control access to websites by risk category, such as dangerous websites, malware-hosting websites, illegal websites, or inappropriate websites. Websites or domains exhibiting security risk behaviors such as phishing, botnet activity, or malware hosting must be blocked automatically.
2) Website access must be for business or operational purposes only.
3) Websites unrelated to work, such as gambling, pornography, copyright-infringing file sharing, or content that poses a reputational risk to the organization, must be blocked.

Part 4.7 Use of Cryptography

Objective

To establish guidelines and measures for the use of cryptographic technology to maintain the Confidentiality, Integrity, and Availability of the organization's data, and to prevent unauthorized access to data.

4.7.1. Use of Cryptography

1) General Use of Cryptography
   - Critical data and personal data must be encrypted both at rest and in transit as required.
   - Internationally accepted encryption methods and algorithms must be used, such as AES, RSA, or SHA-2, or algorithms defined by the organization. The use of outdated or vulnerable encryption methods such as DES, 3DES, MD5, or RC4 is prohibited.
   - Where encryption cannot be applied, alternative protective measures must be used, such as data masking, tokenization, or strict access controls.

2) Data at Rest Encryption
    - Storage devices such as servers, storage systems, laptops, and mobile devices must use full-disk encryption.
    - Critical data or data classified at a sensitive level must be encrypted prior to storage in cloud systems or on portable devices.
    - Storing critical or confidential data on unencrypted media such as unprotected USB drives is prohibited.
    - Backup copies should be encrypted before storage or transfer.
3) Data in Transit Encryption
    - Data transmitted across both internal and external networks must be encrypted using secure protocols such as TLS 1.2 or higher, HTTPS, SSH, or IPsec.
    - File transfers must use encrypted channels such as SFTP, FTPS, or a secure VPN.
    - Transmitting critical data through unsecured channels such as unencrypted email or unauthorized messaging platforms is prohibited.

4.7.2. Cryptographic Key Management

1) The organization shall maintain a key management system or process covering key generation, storage, distribution, rotation, and destruction.
2) Encryption keys must be stored in secure locations such as Hardware Security Modules (HSM), Key Management Services (KMS), or Key Vaults.
3) Key rotation schedules must be defined, and keys must be changed when security risks are identified, such as key leakage, unauthorized access, compromise of key storage systems, or when the encryption algorithm in use is found to have security vulnerabilities.

Part 4.8 System Acquisition, Development and Maintenance

Objective

To minimize errors in requirements definition, design, development, and testing of newly developed or enhanced information systems, and to ensure that developed or procured systems comply with defined agreements.

4.8.1. Secure Development Life Cycle :SDLC

1) The organization shall incorporate security principles into every phase of development, including:
    - Requirement Analysis
    - System Design

- Development
- Testing
- Deployment
- Maintenance

Security risks and necessary controls must be identified from the outset of each project.

2) Secure Architecture and Design
   - Secure-by-Design principles should be applied, such as data layering, access controls, injection prevention, and appropriate authentication, to ensure that systems have a secure architecture from the design phase.

4.8.2. Security Requirements of Information Systems

1) Information Security Requirements Analysis and Specification
   - The IT system development unit, IT project management unit, and units assigned to develop or procure information systems must clearly define information security requirements for all systems to be developed or procured.
   - The IT system development unit, IT project management unit, and units assigned to develop or procure information systems must monitor system development to verify that it meets both information security requirements and the defined functional requirements.
   - Security requirements, performance requirements, and legal and regulatory requirements must be fully considered at both the overall system level and the component level, to ensure that system design and development is secure, efficient, and compliant with all applicable requirements.

4.8.3. Security in Development and Support Processes

1) Secure Development
   - The Digital Technology Department shall establish rules for the secure development of information systems, covering the entire system development lifecycle.
   - Code development must comply with the organization's defined Secure Coding standards, including OWASP Top 10 guidelines, and must address common vulnerabilities such as injection, Cross-Site Scripting (XSS), broken access control, CSRF, insecure deserialization, and improper input validation.

- Critical data must be handled securely. Embedding sensitive information such as passwords, API keys, tokens, or credentials directly in source code is strictly prohibited. Additional protective measures such as encryption or masking and tokenization must be applied in accordance with the sensitivity level of the data.
- Source code must undergo vulnerability scanning using organization-defined tools to assess risks from code, libraries, and open-source components. Any identified vulnerabilities must be remediated in accordance with the organization's defined severity levels.
- Source code must be stored and managed through an organization-approved version control system such as Git, with access rights and merge approvals defined in accordance with Segregation of Duties (SoD) principles. All code must undergo a code review by designated reviewers before deployment.

2) Secure System Engineering Principles
   - The IT system development unit, IT project management unit, and units assigned to develop information systems must adhere to the following security engineering principles as a minimum:
     - Least Privilege: Grant users the minimum access necessary to prevent unauthorized modification of data or systems.
     - Need to Know: Grant users access only to information required for their work to prevent leakage of critical information.
     - Defense in Depth: Design systems with multiple layers of protection to reduce the risk of unauthorized data access.
     - Open Design: Develop systems using standardized, auditable mechanisms and algorithms.
3) Secure Development Environment
   - The IT system development unit, IT project management unit, and units assigned to develop information systems must control the security of the development and integration environment, protecting data generated during development, data transmission, backups, and access to information systems.

4.8.4. Outsourced Development

1) The Digital Technology Department shall establish written agreements for software development by external parties engaged to develop software for use within the organization.

2) The unit assigned to engage external parties for information system development shall regularly supervise, monitor, and track development activities carried out by external parties to prevent any incidents that may adversely affect information security.

4.8.5. System Security Testing

1) The IT system development unit, IT project management unit, assigned units, and users shall jointly test the functional and information security features of all newly developed or modified information systems.
2) Information system development testing must be conducted during development and prior to deployment to the production environment. Evidence of testing for newly developed or modified systems must be formally retained.
3) System Acceptance Testing
    - The Digital Technology Department shall define acceptance criteria for new or enhanced information systems, whether developed internally or procured from external parties, and shall test such systems prior to deployment to the production environment.

4.8.6. Separation of Development, Testing and Operational Environments

1) The Digital Technology Department shall ensure that computer systems are separated into distinct Development, User Acceptance Testing, and Production environments. The Digital Technology Department shall control access rights for each environment and designate personnel clearly responsible for system shutdown activities. Operational results must be reported to supervisors, and any issues encountered must be logged with resolution details and reported to supervisors accordingly.
2) The Digital Technology Department shall control access rights across all environments and designate personnel responsible for system shutdown, with operational reporting to supervisors and logging of all issues and resolutions.

4.8.7. Test Data

1) Protection of Test Data
    - The IT system development unit, IT project management unit, and assigned units shall select test data carefully to ensure security and the reliability of test results, and shall avoid using production data from live systems for testing purposes.

- Controls must be implemented to ensure the secure use of test data, with access restricted to authorized personnel only. Where copies of production data are used for testing, such data must be subject to the same controls as production data.

4.8.8. System Change Control Procedures

1) The Digital Technology Department shall establish written change control procedures covering the entire information system development lifecycle.
2) Technical Review of Applications after Operating Platform Changes
   - System administrators must perform technical reviews to analyze the potential impact of changes or upgrades to operating systems, such as version upgrades and security patches, and must conduct testing in the test environment until it is confirmed that all systems processing on that platform operate normally and securely before applying changes to the production environment.
   - System administrators must conduct post-change technical reviews on the production environment to verify that changes have not adversely affected system operations or information security.

Part 4.9 Change Management Policy

Objective

To establish guidelines for managing information system changes, minimize errors in change implementation, and ensure that systems continue to support the organization's business operations effectively and without disruption.

4.9.1. Change Management

1) The Digital Technology Department shall ensure that changes to information systems that affect information security are subject to change control management.
2) The roles and responsibilities of all parties involved in the change control process must be clearly defined.
3) The Digital Technology Department shall define change types to facilitate the recording, classification, assessment, and approval of change requests. Approving authorities shall be defined as unit managers or above, or persons designated with approval authority.
4) The Digital Technology Department shall establish written operational procedures for information system change management and shall maintain records of all changes.

5) The requester and implementer of any change must conduct an impact analysis and risk assessment, and prepare contingency measures for each change activity.
6) The change requester must develop an overall implementation plan specifying the proposed dates, times, and required resources, and shall notify all relevant parties of the change plan.
7) The change implementer must prepare a Fallback Plan to restore the system to its previous state in the event that a change cannot be successfully completed as intended.

Part 4.10 Protection of information systems during audit testing

Objective

To limit the impact of audit activities on the organization's operations or business activities.

4.10.1. Information Systems Audit Considerations

1) Information System Audit Controls
    - The Digital Technology Department shall develop an information system audit plan aligned with the assessed risks, such as a Vulnerability Assessment plan.
    - The Digital Technology Department shall notify all relevant units prior to conducting any information system audit.
    - The Digital Technology Department shall define the scope of technical audit tests to cover key risk areas, and shall ensure that such audits do not disrupt normal operations. Where an audit may affect system availability, testing must be scheduled outside of business hours.
    - Internal auditors are responsible for preparing audit plans and objectives and submitting them to the auditees, so that the audit plan is agreed upon between the auditor and the auditee, helping to minimize the impact of audit activities on operations or business activities.

Section 5: Artificial Intelligence Governance Policy

Objective

To establish principles and measures for the development, use, management, and governance of the organization's Artificial Intelligence (AI) technology in a manner that is safe, transparent, ethical, legally compliant, and minimizes the risk of adverse impacts on the organization, users, and society.

5.1. The organization shall ensure that the development and use of Artificial Intelligence (AI) technology is focused on delivering benefit (Beneficence) to users, the organization, and society. A value assessment and positive impact evaluation must be conducted prior to deploying AI in any process, such as supporting more accurate decision-making, improving operational efficiency, or understanding customer behavior to enhance service delivery and marketing. The use of AI must not cause harm or negative impact to any individual, such as privacy violations, discrimination, bias, or information security risks.

5.2. Internal company data, whether confidential or not yet publicly disclosed, must not be used with AI systems without authorization from a supervisor.

5.3. 5.3 Applicable laws, regulations, and rules must be taken into account when AI is used as part of the organization's personal data processing. Such use must comply with data privacy requirements such as the General Data Protection Regulation (GDPR) in Europe and the Personal Data Protection Act (PDPA) in Thailand.

5.4. 5.4 The organization shall establish governance to ensure that AI decision-making is transparent, auditable, free from bias, and subject to clearly defined accountability. AI outputs must be regularly tested, reviewed, and monitored, with designated Human Oversight responsible for cases where AI has a significant impact on the organization's operations or decision-making.

Disciplinary Penalties

In order to maintain orderly conduct among employees and to ensure fairness in disciplinary proceedings, the Company establishes disciplinary penalties based on the severity of each offense in accordance with the Company's Employee Regulations. As these regulations may not cover every possible situation, the determination of disciplinary penalties shall be at the Company's discretion, with due consideration for fostering good labor relations and ensuring fairness and equality for all employees.

Annex 1: Supalai Partner Code of Conduct

Supalai Partner Code of Conduct

Supalai Public Company Limited ("the Company") and its subsidiaries (collectively referred to as "Supalai") are fully committed to conducting business in a manner that achieves sustainable growth alongside social and environmental responsibility. The Company places great importance on supply chain management and its tangible implementation through the governance of Supalai's partners. Partners' adherence to this Code of Conduct reflects their commitment to collaborate and advance together with Supalai, promoting sustainable business conduct between partners and Supalai.

The Code of Conduct refers to the specification of fundamental ethical requirements and business conduct requirements of Supalai for its partners, with the aim of encouraging and promoting ethical operations, social responsibility, occupational health and safety of employees, and a commitment to sustainable environmental management.

Partners are responsible for taking actions to ensure that all directors, officers, employees, agents, representatives, suppliers, contractors, and other business partners understand and are obligated to comply with the requirements set out in this Code of Conduct, covering risk management, risk mitigation, and the establishment of control guidelines, with concrete mechanisms for monitoring progress on these matters. Partners agree to notify Supalai in writing if they become aware of or suspect any violation of this Code of Conduct.

1. **Business Ethics and Transparency**

1.1. Anti-Bribery and Anti-Corruption

Partners shall compete fairly on the merits of their own products and services. Partners must not offer, promise, or provide any benefit or item of value, whether directly or indirectly (including but not limited to gifts or business courtesies), with the intent or effect of influencing any person to perform their duties improperly or to grant an unfair advantage to Supalai, the partner, or any other party. Partners shall comply with this requirement and shall ensure that their employees, agents, and contractors do likewise.

1.2. Fair Business Practices

Partners shall not engage in any conduct that constitutes unfair competition, whether on behalf of Supalai, the partner, or any other party. Partners must not engage in bid rigging, price fixing, or the allocation or exchange of customers; must not disclose competitively sensitive information of Supalai, the partner, or any other party to competitors of Supalai or competitors of the partner; and must not abuse any dominant market position, whether for their own benefit or the benefit of others, by refusing to trade fairly, engaging in predatory or discriminatory pricing practices, imposing tying conditions on the sale or supply of goods or services, or engaging in similar improper tactics. Partners must not engage in deceptive or otherwise unfair marketing practices, whether on behalf of Supalai, the partner, or any other party. Partners must not make

false statements about the goods or services of Supalai, the partner, or any other party, nor disparage competitors of Supalai or of the partner, or their goods or services.

1.3. Confidentiality, Data Protection, Personal Data Protection, and Record Keeping

Partners shall maintain confidentiality, protect data, and safeguard personal data using adequate and appropriate security measures to protect data and restrict access to personal data, including mitigating risks of accidental destruction, loss, alteration, or unauthorized disclosure. Partners shall maintain accurate and complete records to ensure accountability, and must not alter or omit any records in order to conceal or misrepresent recorded information, events, or transactions. Records must be retained and disposed of appropriately.

1.4. Conflicts of Interest

Partners shall avoid any situation that may give rise to a perceived conflict of interest. Partners must not enter into any business arrangement with any director, employee, or agent of Supalai that may result in improper conduct toward Supalai.

2. Quality Standards and Business Continuity

2.1. Quality Standards: Partners shall deliver products and services in accordance with agreed specifications and requirements, and shall cooperate with Supalai in the development and improvement of product and service quality.

2.2. Business Continuity : Partners shall maintain a business continuity plan to ensure the continued delivery of products and services to Supalai, both in cases where Supalai's demand for products and services increases and in cases where the partner's operations are disrupted by production interruptions.

3. Human Rights

3.1. Equal Treatment : Partners shall respect the diversity of employees, customers, and others with whom they interact, and must not discriminate on the basis of personal characteristics such as race, color, religion, national origin, gender, sexual orientation, gender identity, age, disability, or any other personal characteristic, including political affiliation.

3.2. Safe and Secure Workplace : Partners shall provide a safe and secure workplace for all their employees and shall prevent accidents involving employees, customers, and visitors. Partners' management shall ensure that this commitment is upheld at all premises and facilities where the partner operates.

3.3. Working Hours, Compensation, and Benefits : Partners shall compensate employees fairly, strive to be ethical employers, and respect employee participation, fair remuneration, and all benefits to which employees are entitled.

3.4. Treatment of Personnel : Partners shall respect the rights of employees and ensure that no harsh or inhumane treatment occurs, including physical, verbal, or psychological abuse or intimidation.

3.5. Freedom of Association : Partners shall respect the rights of employees and provide freedom of association and collective bargaining.

3.6. Protection Against Child Labor : Partners shall protect against the use of forced child labor, illegal labor, or labor that is hazardous and detrimental to the health, morality, and mental well-being of children.

4. Occupational Health and Safety

Partners shall provide a safe and hygienic working environment and protect their employees from potential safety risks by: (1) providing personal protective equipment for workers in hazardous conditions; (2) encouraging employees to report work-related injuries; (3) classifying and recording work-related injuries and illnesses; (4) providing necessary medical treatment; and (5) investigating and implementing corrective measures to eliminate the causes of such injuries and illnesses.

5. **Environment and Sustainability**

Partners shall endeavor to minimize adverse impacts on communities, the environment, and natural resources in order to protect the health and safety of the general public, by establishing measures to prevent and reduce environmental impacts and to reduce greenhouse gas emissions that contribute to climate change.

6. **Social Responsibility and Community Care**

Partners shall demonstrate care and consideration by organizing or participating in activities that constructively engage with communities, with the aim of sustainably developing community and social well-being.

7. **Contact Channels**

Supalai has established channels for employees and stakeholders (including partners, subcontractors, and their employees) to make inquiries and raise concerns regarding this Code of Conduct and business practices through Supalai's ethics helpline, which is a confidential channel that allows concerns to be raised anonymously. Supalai's ethics helpline is available through the following channel: Anti-corruption@supalai.com

8. **Acknowledgment of Compliance with Supalai's Code of Conduct**

Partners acknowledge and agree that they are fully responsible for complying with this Code of Conduct, in order to promote concrete and collaborative supply chain management development and to foster sustainability for both partners and Supalai. Accordingly, Supalai will assess compliance with this Code of Conduct from the date of signing, including through surveys of partner premises and requests for credible evidence demonstrating that the partner complies with this Code of Conduct.

Partners shall cooperate fully with Supalai in such assessments and shall take immediate corrective action if any non-compliant practices are identified. In cases of non-compliance, Supalai may require regular audits by an independent auditor selected by Supalai. Partners agree to such audits and accept responsibility for the costs incurred.

The partner acknowledges, consents, and signs with company seal.

I,_____ , authorized signatory director

of _____hereby agree to comply with the above Code of Conduct.

Signature: _____

Date: _____/____/

Company Seal

Annex 2: IT and Cyber Security Risk Assessment Form for External Contractors

SUPALAI

IT and Cyber Security Risk Assessment Form

For External Contractors

Part 1: External Contractor Details	**Assessment Date:**.....
External Contractor Name:	....
Type of Access Group to Company Data:	☐ IT service provider ☐ Party with access to critical data or customer data of the Company ☐ Party with access to the Company's internal systems, such as CM / CRM systems or others ☐ Other:.....
Details of work performed for the Company:	
(1) Name: ..... Position: ..... Phone: ..... E-mail: ..... Signature: ..... Assessor	
(2) Name: ..... Position: ..... Phone: ..... E-mail: ..... Signature: ..... Assessor	

Part 2: For External Contractors to Assess Their Own Business Risk

Please mark / or fill in the answer and provide additional details where applicable.

Assessment Topic	Assessment Details	Response and Supporting Details
① **IT Security Policy / Measures** (To ensure that the company has adequate, efficient, and effective IT risk management)	1.1 At least one director or advisor who meets any of the following qualifications: - Holds an educational degree in IT - Has knowledge or experience in IT - Has a record of IT training or seminars in the most recent year, such as cybersecurity awareness training	
	1.2 Has established an IT Security Policy / Procedure	
	1.3 จัดให้มีแผนบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT Incident Response Plan) หากเกิดการบุกรุกโจมตีหรือการรั่วไหลของข้อมูลอย่างทันท่วงที	
② **Basic Security / Cyber Security Risk Management Procedures**	2.1 What Cyber Security risk prevention tools are in place? - Antivirus - Firewall - VPN - Patch installation	
	2.2 What methods are used to control access to the company's internal data? (Data Access Procedure) For example: - Designating an approving authority for data access, requiring approval prior to granting access - Defining authentication methods - Defining access rights and maintaining access logs (Authentication, Authorization, and Accounting)	
③ **Significant Cyber-Attack or Information Technology System Incident History**	3.1 Company's data breach history	

Assessment Topic	Assessment Details	Response and Supporting Details
	3.2 History of intrusions or attacks by computer viruses, ransomware, and malware in the most recent yea	Please specify: ○ No intrusion or attack detected ○ Intrusion or attack detected but successfully prevented by the company's detection systems, such as Firewall, Antivirus, Gateway, or Proxy ○ Computer virus detected on user devices, such as through the computer's Antivirus system ○ Computer virus detected on organizational servers (excluding Gateway) ○ Computer virus detected but the source is unknown or cannot be identified ○ Other (please specify): ....
	3.3 History of complaints or incident reports related to cyber threats from stakeholders in the most recent year, such as account theft or personal data leakage, and the remediation measures taken	Please specify: ○ No such history ○ History exists (please specify the incident and number of complaints or reports in the most recent year): ....
④ **Cloud or Hosting Service Usage**	4.1 Type of Cloud Service or Hosting Service used by the company.	Please specify: ○ Not in use (skip to item 5) ○ Private Cloud or Hosting Service or affiliated company ○ Public Cloud, Hybrid ○ Other (please specify): ....
	4.2 Number of critical systems or applications used for processing or supporting company activities that reside on Cloud or Hosting Services, the disruption of which would impact business operations.	Please specify the number of critical systems or applications: System (1):..... System (2)..... System (3).....

Assessment Topic	Assessment Details	Response and Supporting Details
		Please specify the name of the Cloud Provider / Hosting Service in use: ....
⑤ **External Service Providers with Access to the Company's Network or Internal Systems (Third Parties, Vendors, Outsourcers, Sub-Contractors)**	5.1 Are employment contracts established that specify conditions or agreements covering information security responsibilities related to IT Policy, such as specifying the requirement for a Non-Disclosure Agreement between the organization and external contractors?	
	5.2 Number of external service providers with access to the company's internal network (Third Parties, Vendors, Outsourcers, Sub-Contractors).	Please specify the number of external service providers and the type of services used: ○ Number of service providers: ..... ○ Type of service: No. 1 ..... No. 2 ..... No. 3..... No. 4.....
	5.3 Methods or channels through which external service providers access the company's network or internal resources.	Please specify: ○ Service providers must access on-site only ○ Service providers may access through dedicated channels such as Leased Line or VPN ○ Other:..... ....
	5.4 Sub-contractor management guidelines, such as: ○ Notifying the organization when a sub-contractor is engaged or changed	

Assessment Topic	Assessment Details	Response and Supporting Details
	○ Responsibilities of the service provider in cases where sub-contracting is used	
⑥ **Damage Indemnity**	6.1 Does the company have insurance coverage for damages arising from cyber threats?	
⑦ **Training / Awareness**	7.1 Has a training plan been established to raise awareness and provide knowledge to employees, contractors, external service providers, or other relevant parties, such as regular training on IT security policies and procedures?	
⑧ **IT Audit by an Independent and Internationally Accredited External Auditor**	8.1 Has an external auditor been engaged to audit IT operations and internal controls?	Audit standards: ○ SSAE 18 (SOC 2 Type 2 Report) ○ PCI-DSS Attestation of Compliance (AOC) ○ Other (please specify)..... ....