PRECISE

Information Technology Policy

Effective from 13 November 2025

Table of Contents

Section 1: Executive Summary

Precise Corporation Public Company Limited recognizes the importance of enhancing organizational performance through the adoption of information technology as a key resource to strengthen operational capabilities. The application of information technology serves as a guideline for developing efficient IT systems, enabling effective use of information to achieve the organization's missions across various functions. This supports management policies, as well as national policies on information and communication technology development, and facilitates coordination and collaboration with related organizations. As a result, information can flow rapidly within a structured, systematic, and well-organized management process, reducing redundancy, improving customer satisfaction, and continuously developing existing resources to maximize their value. This is achieved while ensuring security and establishing a sound framework for information technology governance.

Therefore, the Company recognizes that the implementation of information technology in its operations requires clearly defined development guidelines to ensure sustainable growth aligned with the organization's strategies and vision, as well as with relevant laws, regulations, and international standards. These guidelines can be practically implemented with efficiency and effectiveness, supporting continuous development in accordance with the organization's objectives.

Section 2: General Provisions

2.1 Objectives

The objectives of this Information Technology Policy are to establish clear guidelines for information technology operations and data management within the organization, and to provide a standardized operational framework for all parties involved with the organization's information assets. This includes executives, employees, internal users, external organizations, and third parties. The policy also aims to define appropriate preventive measures to control and reduce potential damage arising from incidents in which information assets become unavailable, lost, damaged, defective, or compromised in terms of information security.

2.2 Applicable Laws and Regulations

2.2.1 Computer Crime Act B.E. 2550 (2007) and Amendment (No. 2) B.E. 2560 (2017)

2.2.2 Copyright Act B.E. 2537 (1994) and Amendments (No. 2) B.E. 2558 (2015), (No. 3) B.E. 2558 (2015), and (No. 4) B.E. 2561 (2018)

2.2.3 Personal Data Protection Act B.E. 2562 (2019) and Amendment (No. 2) B.E. 2564 (2021)

2.2.4 Royal Decree on Secure Electronic Transaction Procedures B.E. 2553 (2010)

2.2.5 Ministry of Digital Economy and Society Notification on Criteria for Retention of Computer Traffic Data by Service Providers B.E. 2564 (2021)

2.2.6 Electronic Transactions Commission Notification on Information Security Policies and Practices for Government Agencies B.E. 2553 (2010) and Amendment (No. 2) B.E. 2556 (2013)

2.2.7 Electronic Transactions Commission Notification on Information Security Standards for Secure Electronic Transactions B.E. 2555 (2012)

2.2.8 Cybersecurity Act B.E. 2562 (2019)

2.3 Enforcement and Disciplinary Actions

This Information Technology Policy shall take effect from the date of its official announcement and shall apply to all information system users of Precise Corporation Public Company Limited and its subsidiaries without exception. Any employee or staff member who intentionally or negligently violates this policy, regardless of whether damage has occurred, shall be subject to disciplinary action in accordance with the Company's regulations. The Company reserves the right to pursue civil and/or criminal action in accordance with applicable laws, regulations, and announcements.

2.4 Policy Communication

The Information Technology Department is responsible for announcing and disseminating this policy to all information system users within the organization to ensure awareness of individual responsibilities in the use of information technology and the protection of the Company's information assets.

2.5 Policy Review

This Information Technology Policy shall be reviewed and updated at least once a year, or whenever there are significant changes in the business environment, laws, regulations, or technology. The Information Technology Department is responsible for conducting the review, under the supervision of the Information Technology executive, to ensure ongoing relevance and effectiveness.

Section 3: Definitions

This Information Technology Policy defines the following terms to ensure consistent understanding and accurate reference throughout this policy document.

Terminology	Definitions
Organization	Precise Corporation Public Company Limited and its subsidiaries.
Subsidiary	A company over which Precise Corporation Public Company Limited has controlling authority.
Information Technology Department	The Data & Artificial Intelligence (AI) Capital unit under the Digital and Automation Transformation Office, responsible for supporting, promoting, and managing the organization’s information technology operations.
Managing Director	The Managing Director of the Company.
Division Manager	The highest executive responsible for each division.
Section Manager	The highest executive responsible for each section.
Authorized Person	An executive at division level or above, or a person delegated with decision-making authority.
Administrator	An Information Technology staff member assigned responsibility for administering and maintaining information systems or computer networks, including troubleshooting system issues, with authorized access to programs or networks for management purposes.
Personnel	Employees of Precise Corporation Public Company Limited and its subsidiaries.
External Person	Any individual or employee of an external organization who communicates with and has access to the organization’s information assets.
External Service Provider / Third Party	Vendors, business partners, service providers, outsourced personnel, or any individual or legal entity, domestic or international, providing information technology services under a contract or agreement with the organization. This includes subcontractors authorized to access premises or information assets and to use the organization’s information systems within their assigned responsibilities.

Terminology	Definitions
User	Internal personnel, external persons, or external organizations who use the organization's computer systems.
Project Owner	An internal department of Precise Corporation Public Company Limited or its subsidiaries responsible for managing projects that involve engaging external service providers.
Asset Owner / Data Owner	An individual, department, or division that owns or is responsible for information assets or data, and bears the highest impact in the event of data damage or disclosure.
Data	Text, messages, documents, audio, or any information capable of conveying meaning, presented in numeric, linguistic, visual, or symbolic form, whether processed or unprocessed, in electronic or physical media. This includes computer data under the Computer Crime Act and electronic data under the Electronic Transactions Act.
Electronic Data	Data created, sent, received, stored, or processed electronically, such as through electronic data interchange, email, telegraph, telex, or facsimile.
Computer Data	Data, messages, commands, instruction sets, or any other items residing in a computer system that can be processed by such system, including electronic data as defined under electronic transaction laws.
Dataset	A collection of data aggregated from multiple sources and organized according to specific characteristics, structure, or intended use.
Data Catalog	A document listing dataset classified and organized by grouping or categorizing data under the control or possession of the organization.
Data Governance	The establishment of rights, duties, and responsibilities of stakeholders across all stages of data management to ensure data is acquired and used accurately, completely, up to date, securely, and with respect for privacy, while enabling effective interoperability.

Terminology	Definitions
Data Category	Classifications of data such as personal data, confidential organizational data, and similar categories.
Data Classification	The categorization of data based on confidentiality requirements to define access rights and permitted usage. Five classification levels are defined: Public, Internal Use, Confidential, Highly Confidential, and Strictly Confidential.
Data Life Cycle	The sequence of stages through which data passes, from creation to disposal.
Master and Reference Data	Data managed to enable shared access across departments from a single authoritative source, with defined standards to reduce redundancy and improve quality. • Master Data: Internally created and frequently updated data with detailed attributes, such as employee, customer, vendor, product, service, and location data. • Reference Data: Standardized data commonly used across organizations globally, such as postal codes, country codes, and measurement units.
Username or User Account	A set of credentials used to identify a user, define access rights, and impose access restrictions within information systems.
Password	A sequence of characters used for authentication to control access to information systems or data.
Privileged Access	Access rights exceeding those of standard users or administrators, such as root or system administrator privileges.
Information System	Computer systems, data storage systems, email systems, data communication systems, communication devices, printers, scanners, or any related equipment owned by the organization or legally authorized for organizational use.
Information Security	The protection of information in terms of confidentiality, integrity, and availability, as well as authenticity,

Terminology	Definitions
	accountability, non-repudiation, and reliability, ensuring systems remain secure, safe, and protected against intentional or accidental threats.
Information Security Event	An occurrence that disrupts information system services or degrades service quality, such as server failures, email outages, or abnormal system performance.
Information Security Incident	An unwanted or unexpected situation that may result in system intrusion, attack, or compromise of information security.
Vulnerability	A weakness or deficiency in information assets arising from design, implementation, or management flaws that may be exploited by threats, such as software vulnerabilities enabling unauthorized access.
Security Awareness	Education and awareness activities aimed at increasing personnel understanding of information security threats and issues.
Data Backup	The process of copying data to preserve it for recovery in case of modification, loss, or damage.
Source of Data and Information	Repositories or storage locations of data or information in various forms, including specific or centralized data sources.
Information Assets	1. Information technology equipment and peripherals 2. Software, application systems, and related programs 3. Data, information, electronic data, computer data, and intellectual property
Secure Area	Designated locations for housing information system equipment, including: 1. Patching Room 2. Computer Operation Rooms 3. Data Center
Computer Operation Area	Areas used for data input, report generation, and operational information system activities.

Terminology	Definitions
Patching Room	Areas for storing network and telephone connection equipment on each floor.
Data Center	Facilities housing critical computing equipment and servers supporting core information systems
Logs	Records of system usage, processing activities, and security events used for performance monitoring and anomaly detection.
Monitoring	Continuous observation of information systems through log analysis to detect unauthorized access, misuse, or system issues.
Risk	The likelihood of error, loss, leakage, waste, or undesirable events occurring under uncertain conditions, potentially impacting organizational objectives.
Malicious Code or Malware	Software designed to harm system performance or security, such as viruses, worms, and Trojan horses.
Business Continuity Plan (BCP)	A plan to maintain critical business operations and prevent disruption caused by environmental threats, security incidents, or other risks.
Disaster Recovery Plan (DRP)	A preparedness and response plan for emergencies, including relocation of operations and use of backup systems.
Fallback Plan	A plan to revert systems to the most recent stable operational state if emergency recovery efforts fail.
Recovery Time Objective (RTO)	The targeted duration required to restore services or processes after a major disruption.
Recovery Point Objective (RPO)	The maximum tolerable period of data loss is used to design data backup strategies.
Maximum Tolerable Period of Disruption (MTPD)	The maximum acceptable duration of operational disruption beyond which recovery is no longer feasible.
Service Level Agreement (SLA)	A formal agreement between service providers and service recipients defines service details, performance metrics, targets, and responsibilities.

Terminology	Definitions
Operational Level Agreement (OLA)	An internal agreement between organizational units supporting service delivery in alignment with SLAs.
Underpinning Contracts (UC)	A mutual agreement between the service provider and the system provider/vendor to deliver services to the service recipient in accordance with the Service Level Agreement (SLA).
High Priority Application System	Systems supporting core business transactions or mandatory regulatory reporting.
Development Environment	Information systems simulating production environments for system development.
User Acceptance Environment	Information systems simulating production environments for performance and security testing.
Disaster Recovery Center (DRC)	Backup systems, data, and networks enabling continuity of core operations during emergencies.
Production Environment	Live information systems serving users, subject to strict security and access controls.
Mobile Device	Organization-approved laptops, smartphones, and tablets authorized to connect to organizational information systems.
Storage Media	Electronic devices used for data storage, such as hard drives, flash drives, USB drives, and external hard drives.

Section 4: Roles and Responsibilities

4.1 Chairman of the Board

4.1.1 Approve the Information Technology Policy and any subsequent amendments.

4.1.2 Approve matters related to the Information Technology Policy as proposed by the Board of Directors.

4.1.3 Assume overall responsibility for information security of organizational assets to ensure that the Information Technology Policy adequately covers critical information, aligns with business objectives, and meets user requirements.

4.2 hief Executive Officer, President, and Senior Executive Vice President

4.2.1 Approve operational regulations and any amendments thereto.

4.2.2 Define strategic direction and provide support for the development of the Information Technology Policy and related procedures.

4.2.3 Decide on engagement with law enforcement agencies and investigative authorities when there is suspicion of serious legal violations.

4.2.4 Approve and support information security initiatives and act as key sponsors in promoting information security awareness.

4.2.5 Review, summarize, and submit the Information Technology Policy and any amendments to the Chairman of the Board for approval and official announcement.

4.3 Division Managers (All Divisions)

4.3.1 Appoint asset owners, conduct risk analysis of assets, and manage assets under their responsibility to maintain confidentiality, integrity, and availability.

4.3.2 Define roles and responsibilities for personnel regarding information security practices in accordance with the Information Technology Policy.

4.3.3 Ensure personnel and relevant external parties receive education on the Information Technology Policy and related procedures.

4.3.4 Promote and enforce compliance with the Information Technology Policy, including defining methods for assessing the organization's information security environment

4.3.5 Review and approve information security requirements for systems handling sensitive or critical business data prior to project initiation.

4.3.6 Oversee the execution of confidentiality agreements for internal personnel and external parties, specifying information security requirements and potential contractual violations.

4.3.7 Communicate any changes affecting compliance with the Information Technology Policy and related procedures within their areas of responsibility.

4.3.8 Respond to information security incidents with negative organizational impact, including reputational or operational damage, and report such incidents to senior executives.

4.3.9 Support investigations and propose corrective actions for information security incidents.

4.4 Additional Responsibilities for Information Technology Executives

4.4.1 Analyze, assess, and summarize issues with severe organizational impact, such as vendor contract violations, unauthorized software distribution, disclosure of critical information, or significant website changes, and report findings to senior executives.

4.4.2 Ensure structured information security risk assessments are conducted and business impact analysis processes are applied.

4.4.3 Select and propose appropriate personnel to coordinate with law enforcement and investigative agencies in cases of suspected serious misconduct.

4.4.4 Present Information Technology Policy updates and change reports to senior executives.

4.4.5 Provide guidance on performance measurements to improve service delivery and information security controls.

4.4.6 Review and approve requirements for the use of organizational software and information security controls for sensitive or business-critical information prior to IT project design.

4.4.7 Review and approve information security-related activities at departmental level that may impact the organization.

4.5 Asset Owners

4.5.1 Define data classification levels based on organizational importance and communication changes to relevant stakeholders.

4.5.2 Develop and maintain data classification structures and management requirements.

4.5.3 Specify access control rules for information assets, including user roles and access approval procedures, and communicate changes accordingly.

4.5.4 Assess risks and define standardized controls where business needs conflict with the Information Technology Policy or security standards, ensuring risks remain at acceptable levels.

4.6 Administrators

4.6.1 Develop and document operational support processes and procedures in alignment with the Information Technology Policy.

4.6.2 Maintain confidentiality, integrity, and availability of information systems under their control and enforce appropriate access controls.

4.6.3 Provide technical support to asset owners in implementing appropriate security controls.

4.6.4 Establish information security mechanisms and regularly monitor system access to prevent unauthorized intrusion.

4.6.5 Assist in the selection and evaluation of hardware and software with respect to information security requirements.

4.6.6 Notify asset owners and relevant parties of any suspected or confirmed threats, losses, damage, or policy violations.

4.6.7 Respond to information security incidents, support investigations, and resolve suspected threats or inappropriate activities, reporting outcomes to relevant stakeholders.

4.7 System Developers

4.7.1 Comply with the requirements defined in the Information Technology Policy and relevant standards throughout system design, development, implementation, and maintenance to ensure adequate development controls.

4.8 Information Technology Strategy Management Unit

4.8.1 Develop and maintain the Information Technology Policy to ensure alignment with business operations and applicable laws and regulations.

4.8.2 Develop and update procedures and operational guidelines consistent with the Information Technology Policy and international standards.

4.8.3 Propose policy and procedure updates to IT executives for review and approval.

4.8.4 Communicate the Information Technology Policy and related procedures to all users.

4.8.5 Communicate system audit and network activity monitoring practices to users.

4.8.6 Establish mechanisms to monitor policy compliance and ensure users are aware of information security policies, intellectual property laws, and applicable regulations.

4.9 Legal Department

4.9.1 Provide legal guidance related to regulations and procedures for monitoring and auditing information system usage.

4.10 Internal Audit Function

4.10.1Review and assess implementation of the Information Technology Policy, related procedures, operational processes, and information security standards, including evaluation of internal controls, and report audit results to management.

4.11 Users

4.11.1 Understand and comply with organizational policies, procedures, and operational guidelines.

4.11.2 Sign and adhere to confidentiality agreements.

4.11.3 Use organizational assets responsibly, ethically, efficiently, and in compliance with applicable laws.

4.11.4 Immediately report information security incidents to supervisors and the Information Technology Department and support incident response efforts.

4.12 External Organizations / Third Parties

4.12.1Sign and comply with confidentiality agreements.

4.12.2Adhere to the organization's Information Technology Policy when providing third-party services and take necessary actions to protect information confidentiality and systems.

4.12.3Access information systems strictly within authorized privileges.

4.12.4Treat all information accessed or collected during engagement with the organization as confidential and refrain from disclosure, transmission, modification, or use without explicit authorization.

4.12.5Immediately report information security incidents to the organizational unit responsible for the Information Technology Department and support incident response activities.

Section 5: Information Technology Service Management Policies

5.1 Change Management Policy

Objective

To establish guidelines for managing changes to information systems in order to reduce operational errors and ensure that systems continuously and effectively support business operations.

5.1.1 The Information Technology Department shall define change types for recording, classification, assessment, and approval of change requests. Authorized approvers shall be executives at division level or above, or delegated authorities.

5.1.2 The Information Technology Department shall establish documented procedures for managing information system changes and maintain formal change records.

5.1.3 Users, requesters, and change implementers shall analyze the impact and risks associated with changes and prepare appropriate mitigation measures.

5.1.4 Requesters shall document change requirements, while implementers shall prepare an overall change plan specifying schedules, required resources, and notify relevant stakeholders accordingly.

5.1.5 Change implementers shall prepare a Fallback Plan to restore systems to their previous state if changes fail to achieve intended objectives.

5.2 Business Continuity Management

Objective

To define guidelines for ensuring continuity of information system services during emergencies or information security incidents that may disrupt business operations.

5.2.1 The organization shall maintain backup computers and information systems to support continuous business operations, with decisions authorized by top management.

5.2.2 User departments and the Information Technology Department shall conduct risk assessments and document continuity requirements, including MTPD, RTO, and RPO.

5.2.3 The Information Technology Department shall develop a Disaster Recovery Plan (DRP) aligned with the organization's Business Continuity Plan.

5.2.4 The Information Technology Department shall perform backups of data, documents, software, systems, equipment, and ensure availability of essential personnel to enable rapid recovery following disruptions or disasters.

5.3 Incident and Service Request Management Policy

Objective

To establish procedures for managing incidents, resolving issues, and handling service requests efficiently in order to restore normal operations as quickly as possible.

5.3.1 Incident Management

5.3.1.1 The Information Technology Department shall define criteria for assessing impact, urgency, and priority of incidents.

5.3.1.2 Responsibilities for incident resolution and service request prioritization shall be clearly defined to ensure continuity of operations.

5.3.1.3 All incidents and service requests shall be fully recorded in accordance with documented procedures for analysis, resolution, and reporting.

5.3.1.4 The Information Technology Department shall resolve incidents and service requests promptly in accordance with defined service agreements.

5.3.1.5 Unresolved incidents shall be escalated to appropriate levels to improve response efficiency.

5.3.2 Service Request Management

5.3.2.1 Requests for computers, equipment, or software shall be documented with justification, approved by section-level management or above, and processed in accordance with company approval matrices.

5.3.2.2 Requests for new or enhanced information systems shall be documented as formal projects, approved by division-level management or above, including budget approval.

5.3.2.3 The Information Technology Department shall provide relevant technical, security, and vendor information to support procurement decisions.

5.4 Service Level Management Policy

Objective

To define guidelines for establishing acceptable service level agreements between the Information Technology Department and users.

5.4.1 The organization shall establish the following agreements

5.4.1.1 Service Level Agreements (SLA) between service providers and users

5.4.1.2 Underpinning Contracts (UC) with external service providers

5.4.2 SLAs shall be formally approved by IT executives and representatives from user departments.

5.4.3 IT services shall be delivered in accordance with approved SLAs.

5.4.4 Service performance and trends should be regularly reviewed and improved.

5.4.5 A Service Catalogue covering all approved services shall be maintained and acknowledged by management.

5.4.6 Changes to service requirements, SLAs, or service catalogues shall follow the Change Management process.

5.5 Budgeting and Accounting for Services Policy

Objective

To ensure effective budgeting and cost control for information technology services.

5.5.1 The Information Technology Department shall allocate sufficient budgets and control expenditures efficiently.

5.5.2 Budget planning shall consider direct and indirect costs, IT assets, shared resources, administrative expenses, outsourced services, personnel, insurance, maintenance, licensing, and other related costs.

5.6 Service Reporting Policy

Objective

To provide accurate and complete information for management reporting and decision-making.

5.6.1 Internal departments shall provide operational reports and data to management.

5.6.1.1 Internal departments shall prepare operational performance reports and relevant information that are beneficial to business operations and provide such reports to management. This information shall enable management to make operational decisions efficiently, accurately, and in a timely manner.

5.6.1.2 The Information Technology Department shall maintain data sources, operational results, and related information used for management reporting to ensure that such information remains accurate, reliable, and readily available always.

5.6.2 Report Printing

5.6.2.1 Printed reports shall clearly indicate the name of the publisher, as well as the date and time of printing. Logs of report printing and data export activities shall be maintained. Reports that are no longer required shall be securely disposed of.

5.6.3 Access to Data Sources

5.6.3.1 Users shall request authorization to access data sources from the relevant data-owning department prior to accessing such data. Access rights shall be assigned based on data scope and classified into the following three levels

a) Access to data across all divisions/departments

b) Access limited to a specific division/department

c) Access limited to specific subject matters or relevant data only

5.6.4 Data Quality Control of Data Sources

5.6.4.1 In cases where users request changes to data within data sources, users shall prepare and validate the data in accordance with established procedures, including data cleaning to ensure completeness and accuracy. Such requests shall be formally documented in writing and submitted to the Information Technology Department. Authorized IT personnel shall be responsible for implementing the approved data updates within the database.

5.7 IT Insourcing and IT Outsourcing Policy

Objective

To define requirements and operational frameworks for providing and utilizing IT services securely and efficiently.

5.7.1 Provision of Information Technology Services to Other Parties (IT Insourcing)

5.7.1.1 The Information Technology Department shall establish controls and governance over information technology operations to ensure compliance with business-related requirements of the organization. The Information Technology Department shall provide information technology services exclusively to the organization and its subsidiaries.

5.7.1.2 The Information Technology Department shall establish service charges and fees. Such service charges and fees shall be mutually agreed upon between the service provider and the service recipients. The basis, calculation, and structure of service charges and fees shall be clearly explained, transparent, and justifiable.

5.7.1.3 The Information Technology Department shall establish internal controls and develop documented operational procedures (Operation Procedure Manual). Segregation of duties shall be enforced in accordance with a clearly defined organizational and operational structure.

5.7.1.4 The Information Technology Department shall establish emergency preparedness measures, including emergency response plans and data backup arrangements. Backup schedules shall be defined in accordance with agreements made with service recipients.

5.7.1.5 The Information Technology Department shall perform data backups using appropriate storage media and store such media at locations specifically provided and prepared by the service recipients, or at locations mutually agreed upon. Service-related data of service recipients shall not be disclosed or used for any external parties.

5.7.1.6 The organization shall require service providers to manage service levels in accordance with the Service Level Management Policy as defined in Section 5.4.

5.7.2 The engagement of external service providers for information technology services shall align with the organization’s business strategy and shall ensure continuity, reliability, and accuracy of services provided to customers. The following baseline criteria shall apply to the use of external service providers:

5.7.2.1 Criteria for engaging external service providers shall not conflict with applicable laws, regulations, or requirements issued by government authorities.

5.7.2.2 Guidelines for selecting external service providers shall include evaluation of service reliability and verification of the provider’s capability to deliver services in accordance with agreed service level agreements.

5.7.2.3 Measures for information security and data confidentiality shall be established to ensure accountability, customer protection, and appropriate safeguarding of customer information.

5.7.2.4 External service providers shall be regularly monitored, evaluated, and audited to ensure that services are delivered in accordance with defined objectives and performance targets.

5.7.2.5 Risk management guidelines shall be established for the use of external service providers, covering operational risk, strategic risk, reputational risk, and legal risk. Such guidelines shall be formally documented, appropriate to the criticality of outsourced systems, aligned with the organization’s overall risk management policy, and communicated to all relevant parties for compliance.

5. 7. 2. 6 External service providers are strictly prohibited from using unlicensed or copyright-infringing software in the performance of services for the organization. External service providers shall formally certify in writing their compliance with this requirement.

Section 6: Information Security Policies

6.1 Information Security Policy

Objective

To establish a strategic framework for information security management to ensure effectiveness, efficiency, legal compliance, and rapid recovery from security incidents.

6.1.1 Information Security Management Direction

6.1.1.1 Policy for Information Security

a.) The organization shall establish a written Information Security Policy, which shall be approved by the Chairman of the Board or a senior executive delegated by the Chairman of the Board.

b.) The organization shall communicate and disseminate the Information Security Policy to all users and relevant organizational units and ensure compliance with the policy. Such dissemination shall be conducted in a manner that allows users to easily access and understand the policy.

6.1.1.2 Review of the Policies for Information Security

a.) The Information Technology Department shall review and assess the Information Security Policy in accordance with the conditions specified in Section 2.5.

6.2 Organization of Information Security

Objective

To establish control, governance, and monitoring measures for information security responsibilities across organizational units, and to provide guidelines for controlling the use of mobile communication devices in accordance with the Information Security Policy.

6.2.1 Internal Organization

6.2.1.1 Information Security Roles and Responsibilities

a.) Division-level management shall define and document information security roles and responsibilities for personnel within their respective units in writing, in accordance with the established Information Security Policy.

6.2.1.2 Contact with Authorities

a) The Information Technology Department shall compile and maintain a list of relevant authorities and emergency contacts, such as police stations, fire departments, and emergency response units, for use in emergency situations. Such contact information shall be regularly reviewed and kept up to date

6.2.1.3 Contact with special interest groups

a) The Information Technology Department shall compile and maintain a list of information security expert groups and establish communication channels to receive security-related information. This shall enable timely coordination, information exchange, and assistance in the event of incidents affecting information security. Such contact details should be regularly reviewed and kept up to date.

6.2.2 Mobile Computing and Teleworking

6.2.2.1 Mobile Computing and Communication

a) The Information Technology Department shall establish appropriate security measures to protect mobile communication devices, considering the risks associated with connecting such devices to the organization's computer network and when such devices are used outside organizational premises.

b) All users who utilize mobile communication devices to access the organization's information systems shall comply with the Information Security Policy and strictly adhere to information security requirements.

6.2.2.2 Teleworking

a) All users performing work outside organizational premises shall comply with the organization's Information Security Policy in the same manner as when working within the office.

b) Users who access or process the organization's information while working outside the office, or who connect to organizational systems via a Virtual Private Network (VPN), shall obtain prior authorization from the Information Technology Department, system administrators, information asset owners, and their respective departments, with justified reasons.

c) Users requiring remote access to organizational systems shall obtain prior approval from system administrators.6.2.3 Cyber Attack Testing.

6.2.3 Cybersecurity Penetration Testing

a) The Information Technology Department shall conduct cybersecurity risk assessments through penetration testing against various forms of cyber threats. Test results shall be reported, analyzed, and evaluated to support preventive measures. Such testing shall form part of the organization's cybersecurity protection measures.

6.3 Human Resources Security

Objective

To establish control, governance, and monitoring measures for personnel recruitment prior to employment, personnel management during employment, and personnel management upon termination of employment or changes in job responsibilities.

6.3.1 Prior to Employment

6.3.1.1 Screening

a) The organization shall conduct background screening of job applicants and external parties who are required to provide services within the organization.

6.3.1.2 Terms and Conditions of Employment

a) The Human Resources Department shall ensure that employment contracts, personnel agreements, or contracts with external organizations or individuals include clearly defined information security roles and responsibilities. Personnel and external parties shall acknowledge and accept the organization's rules and regulations, and shall read, understand, and comply with the Information Security Policy, as well as all applicable policies, rules, and regulations established by the organization.

6.3.2 During employment

6.3.2.1 Management Responsibilities

a) Division-level management shall establish controls and oversight to ensure that personnel and external parties engaged to perform work or provide services to the organization comply with the Information Technology Policy and the Information Security procedures formally adopted by the organization.

6.3.2.2 Information security awareness, education and training

a) The Information Technology Department shall provide appropriate channels for personnel and external parties to study and understand the Information Security Policy, as well as their roles and responsibilities related to information security, prior to being authorized to commence work with the organization.

b) The Information Technology Department shall arrange regular training on general operational topics through responsible units, enabling personnel and external parties to continuously learn and understand such topics. These may include system usage, application software operation, basic computer troubleshooting, and compliance with relevant laws, rules, and regulations.

c) The Information Technology Department shall conduct regular information security awareness and training programs to enable personnel and external parties to understand information security requirements, support effective job performance, and ensure secure operations.

6.3.2.3 Disciplinary Process

a) The organization shall establish a disciplinary process to address violations or breaches of the Information Technology Policy, Information Security procedures, or operational processes related to information security.

6.3.3 Termination or Change of Employment

6.3.3.1 Termination or Change of Employment Responsibilities

a) The Human Resources Department shall define, document, and communicate rules, responsibilities, and information security obligations applicable to personnel and external parties upon termination of employment or changes in job responsibilities.

b) The Human Resources Department shall ensure that personnel and external parties strictly comply with the defined rules and obligations.

6.4 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 avoid damage to the organization's information assets.

6.4.1 Responsibility for assets

6.4.1.1 Inventory of Assets

a) The Information Technology Department shall ensure that internal units maintain an inventory of information assets to appropriately manage and control such assets. The asset inventory shall be regularly reviewed and kept up to date.

6.4.1.2 Ownership of Assets

a) The Information Technology Department shall ensure that asset ownership is clearly identified, including designation of asset owners, custodians responsible for controlling asset usage, and individuals accountable for information assets, as appropriate.

6.4.1.3 Acceptable Use of Assets

a) The Information Technology Department shall establish acceptable use requirements for information assets to ensure appropriate management of computer equipment, maximize operational efficiency, and maintain protection against potential damage. Such requirements shall be communicated to organizational personnel, who shall comply accordingly.

6.4.1.4 Return of Assets

a) The Human Resources Department, supervisors, or line managers shall oversee and ensure that organizational personnel or external parties providing services return all organizational assets upon termination of employment or completion of engagement. Such assets include, but are not limited to, laptops, documents, keys, and employee identification cards.

6.5 Access Control

Objective

To establish security practices for controlling access to and use of the organization's information systems, and to prevent unauthorized intrusion through network systems by attackers or malicious programs that may cause damage to the organization's information assets.

6.5.1 Business Requirement for Access Control

6.5.1.1 Access Control Policy

a) The organization shall establish a written Access Control Policy, keep it up to date, and communicate it to internal users to ensure awareness and compliance.

6.5.1.2 Access to Networks and Network Service

a) The Information Technology Department shall require users to request access to data and information systems, subject to approval by division-level management or above.

b) The Information Technology Department shall restrict user access to network services strictly to those services explicitly authorized by division-level management or above. Access rights shall be granted based on job responsibilities and business necessities.

c) The Information Technology Department shall retain computer traffic data (log data) in accordance with the requirements stipulated under the Computer Crime Act.

6.5.2 User Access Management

6.5.2.1 User Registration and De-Registration\

a) The Information Technology Department and data owners shall jointly define, document, and maintain procedures for user registration and de-registration. Such procedures shall be kept up to date and communicated to internal users for compliance.

6.5.2.2 User Access Provisioning

a) The Information Technology Department and data owners shall assign or grant access rights to users for accessing data or information systems based on assigned roles and responsibilities.

b) The Information Technology Department and data owners shall document all access authorization records and retain them as operational evidence.

c) The Information Technology Department and data owners shall define procedures for managing access rights in cases where users require access beyond their assigned privileges.

6.5.2.3 Management of Privileged Access Right

a) The Information Technology Department shall securely store credentials for privileged user accounts, such as server administrator/root accounts or application administrator accounts and grant their use strictly on a need-to-use basis.

b) The Information Technology Department shall establish documented procedures for managing privileged access credentials and communicate such procedures to relevant personnel for compliance.

6.5.2.4 Review of User Access Rights

a) The Information Technology Department and data owners shall establish documented procedures for reviewing user access rights to information systems and applications. Such procedures shall be kept up to date and communicated to internal users.

b) The Information Technology Department and data owners shall clearly define access reviews and communicate them to relevant parties.

c) Access reviews shall consider, at a minimum, the following conditions:

- Defined access review periods
- Termination of employment
- Changes in job roles or responsibilities

d) Upon completion of access reviews, data owners or system administrators shall retain documented evidence of such reviews, organized by each review period.

6.5.2.5 Removal of Access Rights

a) Data owners and system administrators shall define written criteria and procedures for removing access rights and communicating such requirements to internal users for compliance.

6.5.3 User Responsibilities

6.5.3.1 Use of Secret Authentication Information

a) Users shall not use weak or easily guessable passwords, such as dictionary words, combinations derived from usernames, sequential characters, personal information, or predictable phrases (e.g., “nan12345”).

b) Users shall not write down, record, store, or display passwords near systems or devices associated with those passwords.

c) Users shall be accountable for all activities performed using their user accounts. Users shall not allow others to use their accounts, nor perform any actions using accounts for which they are not authorized.

d) Users shall comply with all other password management requirements established by the Information Technology Department.

6.5.4 Application and Information Access Control

6.5.4.1 Information Access Restriction

a) Data owners and system administrators shall define and enforce access methods to information systems and system functions in accordance with the Access Control Policy.

6.5.4.2 Secure Log-on Procedures

a) The Information Technology Department shall establish documented secure log-on procedures based on internationally recognized standards, keep such procedures up to date, and communicate them to internal users for compliance.

6.5.4.3 Use of Privileged utility Programs

a) The Information Technology Department shall control and restrict the use of privileged utility programs for critical information systems or applications to prevent violations of, or circumvention of, established information security controls, as certain utility programs may enable users to bypass security measures.

6.5.4.4 Access control to program source code

a) The Information Technology Department shall establish controls over access to program source code and the use of source code for development purposes to prevent errors or unauthorized changes to the organization’s information systems and applications.

6.6 Physical and Environment Security

Objective

To establish preventive measures, usage controls, and maintenance requirements for physical information assets and information technology equipment that form the infrastructure supporting the organization's information systems, ensuring that such assets remain in a complete and operational condition, and to prevent unauthorized access to information assets or unauthorized disclosure of information.

6.6.1 Secure Area

6.6.1.1 Physical Security Perimeter

a) The organization should identify and establish secure areas, such as computer data center facilities, including the implementation of physical barriers, enclosed areas, walls or perimeter fencing, designated main entry and exit points, and appropriate security systems.

6.6.1.2 Physical Entry Controls

a) The Information Technology Department shall establish physical access controls for secure areas, including computer data centers and system administrator work areas. Access shall be restricted to authorized personnel only. Entry and exit logs for data center facilities shall be maintained and shall include details of individuals, access time, purpose of entry and exit, and such logs shall be reviewed on a regular basis.

6.6.2 Equipment

6.6.2.1 Equipment Setting and Protection

a) The Information Technology Department shall locate information technology equipment in secure rooms or areas. Server cabinets, server racks, and network communication equipment cabinets shall be kept locked at all times. Only authorized personnel shall be permitted to access such equipment for maintenance or reconfiguration purposes to reduce the risk of unauthorized access.

6.6.2.2 Supporting Utilities

a) The Information Technology Department and relevant units shall ensure the installation and maintenance of system failure protection equipment and supporting utilities within computer rooms, including fire suppression systems, smoke detection systems, uninterruptible power supplies (UPS), temperature and humidity control systems, water leakage detection systems, and alert mechanisms for abnormal operation of information technology equipment. Such equipment shall be properly maintained to ensure continuous availability.

6.6.2.3 Cabling Security

a) The Information Technology Department and relevant units shall ensure that the installation and maintenance of electrical and communication cabling within operational areas and computer rooms comply with applicable industrial safety standards in order to prevent unauthorized access, data interception, or physical damage.

6.6.2.4 Equipment Maintenance

a) The Information Technology Department shall ensure that all critical information system equipment used for operational processing, as well as supporting equipment, are maintained in accordance with defined maintenance schedules and manufacturer recommendations to ensure continuous operation and operational readiness.

b) The Information Technology Department shall ensure that maintenance activities, identified issues, and equipment defects are recorded for assessment and improvement purposes, to always maintain equipment in a ready-for-use condition.

6.6.2.5 Removal of Assets

a) Users shall not remove information technology equipment, information assets, or software from the organization’s premises unless prior authorization has been obtained from designated authorized personnel.

6.6.2.6 Unattended User Equipment

a) Users shall lock computer screens or critical devices when not in use or when leaving their workstations unattended.

6.6.2.7 Clear Desk and Clear Screen Policy

a) System administrators shall enforce automatic screen locking mechanisms when systems are unattended, such as session time-outs and automatic screen locks (Clear Screen).

b) Users shall not leave sensitive information, such as paper documents or storage media, in unsecured locations, public areas, or places that are easily visible. Users shall store information assets in appropriate secure locations and apply protective measures to prevent access by unauthorized individuals.

c) Users should store important information on storage locations provided by the organization and shall avoid storing such information on personal computers to prevent unauthorized access.

6.7 Cryptographic Control

Objective

To establish reliable and internationally compliant cryptographic controls by defining secure data encryption methods and implementing effective cryptographic key management. These measures are designed to ensure appropriate and effective preservation of data confidentiality, integrity, and authenticity.

6.7.1 The organization shall define and implement secure encryption methods in accordance with internationally recognized standards.

6.7.2 The organization shall establish cryptographic key management controls covering the entire key lifecycle, including key generation and deployment, secure storage and backup of cryptographic keys, and key revocation or destruction. Encryption keys, storing and backing up encryption keys, and revoking or destroying encryption keys.

6.7.3 The organization shall establish controls over cryptographic keys provided or managed by external parties. Such controls shall be verified to ensure that cryptographic keys generated are not shared with or reused by other parties.

6.7.4 The organization shall establish response procedures to address incidents involving the compromise, leakage, or unauthorized disclosure of cryptographic keys.

6.8 Operations Security

Objective

To establish security controls for operational activities and secure communications management, ensuring that the organization’s information security operations are performed in a structured, well-defined, and secure manner.

6.8.1 Operations Procedures and Responsibilities

6.8.1.1 Documented Operating Procedures

a) The Information Technology Department shall establish documented operating procedures for critical information systems. Duties and responsibilities shall be clearly segregated in accordance with defined operational structures to ensure that personnel perform their duties correctly and in compliance with the organization’s Information Security Policy.

b) Units within the Information Technology Department shall develop operation manuals, system documentation, and knowledge bases to ensure that relevant personnel understand system functions, job responsibilities, and operational processes.

c) Units within the Information Technology Department shall regularly review and update operating procedures, manuals, system documentation, and knowledge bases to ensure they remain current, accessible, and ready for use. Such procedures shall be communicated to relevant personnel for compliance.

6.8.1.2 Change Management

a) The Information Technology Department shall control and govern changes to information systems prior to any modification, correction, or action that may impact system operations, in accordance with Section 5.1, Change Management Policy.

6.8.1.3 Capacity Management

a) System administrators shall monitor the performance of critical systems and information technology equipment to ensure continuous and efficient operation.

b) System administrators shall assess the capacity and adequacy of information resources, including servers, network devices, CPU, memory, storage, and network bandwidth. Capacity planning shall be conducted to ensure that information systems remain sufficient and effective for future operational needs.

6.8.1.4 Separation of Development Testing and Operational Environments

a) The Information Technology Department shall ensure the segregation of development environments, testing environments, and production (operational) environments.

b) The Information Technology Department shall define access rights for each environment and assign responsible personnel for system shutdowns. Operational results shall be reported to supervisors. Any identified issues shall be documented along with corrective actions and reported accordingly.

6.8.2 Protection from Malware

6.8.2.1 Controls Against Malware

a) The Information Technology Department shall implement measures for malware detection, prevention, and system recovery to protect information assets. Appropriate awareness activities shall be provided to users.

b) The Information Technology Department shall promptly communicate information regarding new malware threats or outbreaks. Users who identify suspicious events or risks impacting business operations or information systems shall immediately notify the Information Technology Department.

c) Users shall exercise caution to prevent malware from entering organizational systems, including scanning all removable media from external sources and scanning downloaded files, email attachments, and internet-sourced content prior to use.

d) If users detect or suspect malware infection, they shall immediately disconnect the affected device from the network and refrain from using or reconnecting the device to prevent malware propagation. The Information Technology Department shall be notified immediately.

6.8.3 Backup

6.8.3.1 Information Backup

a) The Information Technology Department shall define backup measures, backup schedules, and perform regular backups of critical information systems to prevent data loss.

b) Users shall be responsible for backing up important data from their computers to company-provided storage media and ensuring data is kept current and securely stored to prevent data leakage.

6.8.4 Logging and Monitoring

6.8.4.1 Event Logging

a) System administrators shall retain sufficient log data related to information security for audit and investigation purposes.

b) System administrators shall monitor information system usage and regularly review monitoring results to detect anomalies, analyze incidents, perform corrective actions, and establish preventive measures to avoid recurrence.

6.8.4.2 Protection of Log Information

a) System administrators shall protect log data and logging systems from unauthorized modification, destruction, or access.

6.8.4.3 Administrator and Operator Logs

a) System administrators shall record activities performed by administrators and operators, including login times, system configuration changes, system errors, and corrective actions. Such logs shall be reviewed regularly.

6.8.4.4 Clock Synchronization

a) System administrators shall ensure that information systems and equipment are synchronized with an accurate and reliable time source aligned with international reference time.

b) System administrators shall regularly verify and update system time settings to prevent incorrect time recording.

6.8.5 Control of Operational Software

6.8.5.1 Installation of Software on Operational Systems

a) The Information Technology Department shall establish procedures and controls for installing software on production systems to restrict user installation and prevent unauthorized software installation.

b) The Information Technology Department shall define and maintain a documented list of approved standard software permitted for installation on organizational computers and communicate such requirements to users for compliance.

6.8.6 Technical Vulnerability Management

6.8.6.1 Management of Technical Vulnerabilities

a) The Information Technology Department shall ensure that technical vulnerability assessments of information systems are conducted at least once per year.

b) System administrators shall maintain systems to preserve information security by conducting vulnerability assessments, evaluating identified risks, and remediating vulnerabilities. This includes user account management and regular antivirus updates.

6.8.6.2 Restrictions on Software Installation

a) Users shall comply with software installation controls and shall not install unlicensed or copyright-infringing software on organizational computers.

6.8.7 Information Systems Audit Considerations

6.8.7.1 Information System Audit Controls

a) The Information Technology Department shall establish information system audit plans aligned with assessed risks, such as vulnerability assessment plans.

b) The Information Technology Department shall notify relevant units prior to conducting any information system audits.

c) The Information Technology Department shall define the scope of technical audits to cover critical risk areas and ensure that audit activities do not disrupt normal operations. Where audits may impact system availability, testing shall be conducted outside normal working hours.

6.9 Communications Security

Objective

To establish control measures for managing computer networks and the transmission of information through internal and external computer networks in a secure manner.

6.9.1 Network Security Management

6.9.1.1 Network Controls

a) System administrators shall control and govern the management of computer network controls to protect against threats and ensure the security of information systems, network-based applications, and information exchanged over the network.

6.9.1.2 Security of Network Services

a) System administrators shall ensure that security requirements, service levels, and management requirements for all network services are defined and documented in service agreements or contracts, whether such services are provided internally or by external service providers.

6.9.1.3 Segregation in Network

a) The Information Technology Department shall implement appropriate network segregation based on user access requirements, potential information security impacts, and the criticality and sensitivity of data residing on the network

6.9.2 Information Transfer

6.9.2.1 Agreements on Information Transfer

a) Any transfer of information between the organization and external parties shall be subject to prior approval from the data owner and shall be governed by documented written agreements.

6.9.2.2 Electronic Messaging

a) The Information Technology Department shall establish controls for electronic messaging systems, such as email, Electronic Data Interchange (EDI), and instant messaging. Important electronic messages shall be appropriately protected against unauthorized access, modification, disruption, or denial of service.

6.9.2.3 Confidentiality or Non-Disclosure Agreements

a) Division-level management shall ensure that personnel and external parties performing work for the organization execute written confidentiality or non-disclosure agreements to protect the organization's information.

6.10 System Acquisition, Development and Maintenance

Objective

To reduce 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 agreed requirements.

6.10.1 Security Requirements of Information Systems

6.10.1.1 Information Security Requirements Analysis and Specification

a) The Information Technology System Development Unit, the Information Technology Project Management Unit, and assigned units responsible for developing or procuring information systems for organizational use shall clearly define information security requirements for systems to be developed or acquired.

b) The Information Technology System Development Unit, the Information Technology Project Management Unit, and assigned units shall monitor system development activities to ensure that information systems are developed in accordance with defined information security requirements and functional requirements.

6.10.2 Security in Development and Support Processes

6.10.2.1 Secure Development Policy

a) The Information Technology Department shall establish rules and regulations for secure system development covering the entire information system development lifecycle.

6.10.2.2 System Change Control

a) The Information Technology Department shall establish documented procedures for controlling system changes throughout the information system development lifecycle.

6.10.2.3 Technical Review of Applications after Operating Platform Changes

a) System administrators shall conduct technical reviews to assess potential impacts when operating platforms are changed or upgraded, such as version upgrades. Testing shall be performed in a test environment until it is confirmed that systems operate normally and securely before implementing changes in the production environment.

b) System administrators shall perform post-implementation technical reviews following operating platform changes in the production environment to ensure that such changes do not adversely affect system operations or information security.

6.10.2.4 Restrictions on Changes to Software Packages

a) Commercial off-the-shelf software used within the organization should be used without modification. Where modification is necessary, assigned units shall apply strict controls over such changes.

b) Any modifications to software packages shall be performed in accordance with the system change control procedures defined by the Information Technology Department.

6.10.2.5 Secure System Engineering Principles

a) The Information Technology System Development Unit, the Information Technology Project Management Unit, and assigned units responsible for system development shall adhere to the following information security principles, at a minimum:

- Least Privilege: Granting users the minimum access rights necessary to perform their duties, to prevent unauthorized modification of data or systems.
- Need to Know: Granting access strictly based on operational necessity to prevent leakage of sensitive information.
- Defense in Depth: Designing systems with multiple layers of security controls to reduce the risk of unauthorized access.

- Open Design: Designing systems using standardized mechanisms or algorithms that are transparent and verifiable.

6.10.2.6 Secure Development Environment

a) The Information Technology System Development Unit, the Information Technology Project Management Unit, and assigned units shall control and secure development and system integration environments. This includes protecting system data generated during development, data transmission, data backup, and access to information systems.

6.10.2.7 Outsourced Development

a) The Information Technology Department shall establish written agreements governing system development activities performed by external parties developing software for organizational use.

b) Units responsible for engaging external development providers shall supervise, monitor, and regularly track outsourced development activities to prevent any adverse impact on information security.

6.10.2.8 System Security Testing

a) The Information Technology System Development Unit, the Information Technology Project Management Unit, assigned units, and users shall jointly test both functional and information security controls of newly developed or modified information systems.

b) Information system testing shall be conducted during development and prior to production deployment. Formal test evidence shall be retained for newly developed or modified systems.

6.10.2.9 System Acceptance Testing

a) The Information Technology Department shall establish acceptance criteria for new or enhanced information systems developed internally or procured from external parties and shall ensure that such systems are tested prior to being placed into production.

6.10.3 Test Data

6.10.3.1 Protection of Test Data

a) The Information Technology System Development Unit, the Information Technology Project Management Unit, assigned units, and users shall avoid using live production data for testing purposes. Where copies of production data are required for testing, such data shall be protected and controlled to the same level as data used in the production environment.

6.11 Supplier Relationships

Objective

To establish requirements and an operational framework for external parties in providing or consuming information technology services, ensuring efficiency, information security, and maximum benefit to the organization.

6.11.1 Information Security in Supplier Relationships

6.11.1.1 Information Security Policy for Supplier Relationships

a) The Information Technology Department shall establish information security policies applicable to external parties. Relevant stakeholders shall assess potential risks and define appropriate preventive measures prior to granting external parties or individuals access to the organization’s information systems or information assets.

b) System administrators and assigned units responsible for coordinating with external parties shall ensure that external parties providing services comply with contractual agreements or service arrangements. Such agreements shall cover information security requirements, service scope, and service level requirements.

6.11.1.2 Addressing Security within Supplier Agreements

a) The Information Technology Department shall ensure that written agreements are established to address information security requirements related to granting external parties access to information systems or information assets for reading, processing, system administration, or system development purposes.

b) System administrators and assigned coordinating units shall ensure that external parties are granted access to organizational information strictly on a need-to-know basis and only with written approval from the information asset owner.

c) System administrators and assigned coordinating units shall ensure that external parties comply with all requirements and agreements established between the organization and such external parties.

6.11.2 Supplier Service Delivery Management

6.11.2.1 Monitoring and Review of Supplier Services

a) System administrators and assigned coordinating units shall regularly monitor and review the operations of external parties responsible for managing information processing systems for the organization. This shall include assessment of the supplier's financial stability, operational processes, and service performance.

6.11.2.2 Managing Changes to Supplier Services

a) In the event that an external service provider changes its processes, procedures, operational methods, or information security practices, system administrators and assigned coordinating units shall conduct a risk assessment of such changes and report the results to management and relevant stakeholders. Appropriate risk management measures shall be defined and implemented in alignment with the identified risks.

6.12 Information Security Incident Management

Objective

To establish guidelines for managing information security incidents, learning from issues and failures, and implementing corrective improvements in order to prevent the recurrence of information security incidents.

6.12.1 Management of Information Security Incidents and Improvements

6.12.1.1 Responsibilities and Procedures

a) The Information Technology Department shall define roles and responsibilities for managing undesirable or unexpected information security situations and clearly assign operational authority to personnel within the department.

b) The Information Technology Department shall classify undesirable or unexpected information security events separately from general operational incidents in order to determine appropriate and effective corrective actions.

6.12.1.2 Reporting Information Security Events

a) Users and external parties shall report any events related to the organization's information security to their supervisors and the Information Technology Department through designated reporting channels as quickly as possible.

6.12.1.3 Assessment of and Decision on Information Security Events

a) System administrators shall assess information security events, categorize and prioritize incidents based on defined criteria, and notify relevant parties for corrective action where incidents are determined to have an impact on information security.

6.12.1.4 Response to Information Security Incidents

a) Personnel assigned to resolve information security incidents and contracted external parties shall follow the established incident response procedures.

b) Assigned personnel and contracted external parties shall respond to and resolve information security incidents within defined timeframes. If resolution cannot be completed within the specified timeframe, supervisors shall be notified as soon as possible.

6.12.1.5 Learning from Information Security Incidents

a) Personnel assigned to resolve information security incidents and contracted external parties shall prepare analysis and resolution reports identifying root causes, weaknesses, or vulnerabilities related to information security incidents. Such reports shall be retained as organizational knowledge to support continuous improvement and reduce the likelihood of recurrence.

6.12.1.6 Collection of Evidence

a) Personnel assigned to resolve information security incidents and contracted external parties shall collect and preserve evidence related to information security incidents in sufficient detail to support reporting to relevant management and for potential legal proceedings.

6.13 Information Security Aspects of Business Continuity Management

Objective

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

6.13.1 Information Security Continuity

6.13.1.1 Planning Information Security Continuity

a) Information asset owners and the Information Technology Department shall jointly identify events that may impact business processes, assess associated risks and critical systems, and obtain accurate and complete information to support the development of information security continuity plans.

6.13.1.2 Implementing Information Security Continuity

a) The Information Technology Department shall develop emergency response and contingency plans incorporating information security controls and ensuring alignment with the organization's Business Continuity Management (BCM) plan.

6.13.2 Redundancies

6.13.2.1 Availability of Information Processing Facilities

a) The organization shall ensure that availability requirements for critical information systems are assessed and documented.

b) The organization shall ensure the implementation of adequate backup systems, redundant equipment, or supporting systems to maintain appropriate levels of business continuity.

6.14 Compliance

Objective

To ensure that the organization's operations comply with applicable laws, agreements, contracts, and information security requirements that the organization and its personnel are obligated to follow, and to enable monitoring and verification of compliance with established information security policies.

6.14.1Compliance with Legal and Contractual Requirements

6.14.1.1 Identification of Applicable Legislation and Contractual Requirements

a) All personnel shall be responsible for strictly complying with identified legal and contractual requirements.

b) Personnel are strictly prohibited from using the organization's information assets and information technology systems to perform any activities that violate the laws of the Kingdom of Thailand, international laws, or public morals under any circumstances. Any such actions shall be deemed outside the scope of the organization's responsibility, and users shall bear sole responsibility for such actions.

c) Personnel are prohibited from using the organization's information assets and information technology systems for commercial activities, profit-seeking purposes, or any activities unrelated to the organization through the organization's computers or networks.

d) Personnel are prohibited from using the organization's information assets and information technology systems in any manner that infringes upon the rights of others. This includes unauthorized access to or modification of data not belonging to oneself, hacking into other users' accounts, developing software or hardware intended to compromise security mechanisms, unauthorized access to the organizations or other entities' computer systems, and publishing or disseminating content that may cause harm, defamation, or damage to others. The use of inappropriate language or content that causes harm to others shall also be considered a violation of individual rights. In such cases, users shall bear sole responsibility, and the organization shall not be liable for any resulting damages.

6.14.1.2 Intellectual Property Rights

a) The Information Technology Department shall establish processes for managing the use of licensed software and intellectual property to ensure that the use of information assets and software complies with applicable laws and contractual requirements.

b) Users shall not copy or distribute licensed software acquired by the organization, except for copies made solely for emergency recovery or backup replacement of the original software.

c) Users are strictly prohibited from using, reproducing, or distributing images, articles, books, or documents that infringe copyright, or from installing unlicensed software on the organization's information systems.

d) Software developed for the organization, whether by external parties or internal personnel, shall be the property of the organization. Unauthorized copying or distribution of such software by external parties or internal personnel is strictly prohibited.

e) Users utilizing software on the organization's information systems shall strictly comply with copyright laws, the Information Security Policy, and software vendor requirements.

f) Employees are prohibited from storing or recording unlicensed music or video files on the organization's information assets, as such actions constitute unauthorized use of copyrighted materials.

6.14.1.3 Protection of Records

a) Information asset owners shall comply with legal requirements applicable to specific types of information, such as accounting and customer data, and shall define information handling and retention periods in accordance with such regulations.

b) The Information Technology Department shall protect log records and evidence from damage, loss, unauthorized modification, access, or disclosure, ensuring that controls align with legal requirements, regulatory obligations, and business needs.

6.14.1.4 Privacy and Protection of Personal Identifiable Information

a) The organization shall ensure the protection of personal data in compliance with applicable laws, governmental regulations, official guidelines, and the organization's Personal Data Protection Policy.

b) Customer information is considered critical. Responsible units shall ensure that only authorized personnel, assigned by job responsibilities or approved by supervisors, are permitted to modify such information.

c) Personal information of personnel, employees, and customers shall be treated as confidential and disclosed only to authorized individuals as defined by the organization.

6.14.2 Information Security Reviews

6.14.2.1 Independent Review of Information Security

a) The organization shall conduct independent information security reviews through internal audit units or external independent auditors to verify compliance with information security policies, standards, and procedures, and to assess the adequacy and effectiveness of information system controls.

6.14.2.2 Compliance with Security Policies and Standards

a) Department heads shall be responsible for regularly reviewing and ensuring compliance with information security policies, standards, and procedures by personnel under their supervision.

b) If non-compliance is identified that does not impact the organization's information security, supervisors shall inform and educate personnel accordingly. However, if non-compliance affects information security, disciplinary actions shall be taken in accordance with organizational regulations.

c) The Information Technology Department shall provide guidance and support regarding compliance with information security policies, standards, procedures, and related requirements upon request from other units.

6.14.2.3 Technical Compliance Review

a) The internal audit function shall review technical controls of information systems to verify their adequacy and compliance with established controls.

b) System administrators shall conduct regular information security testing, such as vulnerability assessments or penetration testing, at least once per year, in accordance with the Information Security Policy and international information security standards.

Section 7: Data Management

7.1 Data Management

Objective

To ensure that data management of Precise Corporation Public Company Limited and its subsidiaries ("the Company") complies with applicable laws and regulations, and to provide a framework and guidelines for data management across organizational units for executives, employees, and relevant stakeholders.

7.2 General Requirements for Data Management

7.2.1 Roles, duties, and responsibilities shall be defined for each individual in accordance with the organizational structure. Such roles shall be formally authorized and approved by management. Data ownership shall be assigned to designated organizational units responsible for managing specific data assets.

7.2.1.1 Department heads or their delegated representatives shall control and oversee personnel within their units, as well as relevant stakeholders, to ensure strict compliance with the Data Management Policy

7.2.1.2 Supervisors shall ensure that personnel within their units and other parties, such as companies or contractors assigned by the unit to perform data management functions, receive appropriate knowledge and understanding of this policy and effectively and efficiently implement it in practice.

7.2.1.3 Personnel within units and other parties, such as companies or contractors assigned to perform data management functions, shall comply with all applicable policies, measures, procedures, and guidelines related to data and information systems as defined by the organization.

7.2.1.4 The Digital and Automation Transformation Office, the Data Governance & Enterprise Information Architecture Team (PDE), data creators, data managers, data owners, and data custodians shall perform their assigned roles and responsibilities in accordance with this policy.

Examples of the definition of roles and responsibilities of relevant stakeholders are as follows.

Role	Responsibilities
Digital and Automation Transformation Office	• Comprises the Vice President – Digital and Automation Transformation Office • Holds the highest authority over data governance within the organization, responsible for policy-level decision-making, issue resolution, and overall data management of the organization • The Chief Information Officer (CIO) or senior IT executive may act on behalf of the Chief Data Officer (CDO), where applicable
Data & Artificial Intelligence (AI) Capital Unit	• Define requirements for data quality and information security • Draft data policies, standards, and data-related guidelines • Monitor and assess compliance with data policies, data quality, and data security, and analyze assessment results
Data Governance & Enterprise Information Architecture Team (PDE)	• Define and manage metadata
Application Software Maintenance and Support Service Team (PDE)	• Provide information technology support to data users • Maintain and manage data residing on the organization's information technology systems

7.2.2 Establish data-related standards and guidelines to support operational activities in compliance with this policy.

7.2.3 Define measures, methods, and practices for ensuring data security in order to prevent unauthorized or unlawful access, disclosure, loss, destruction, or alteration of data.

7.2.4 Define measures, methods, and practices for personal data protection in compliance with applicable laws, regulations, and organizational guidelines, with reference to the Privacy Policy and in accordance with the Personal Data Protection Act B.E. 2562 (2019).

7.2.5 Review the existence and details of critical data, such as data descriptions or metadata, datasets, data classification, and report the results to responsible parties.

7.2.6 Monitor, track, and evaluate compliance with the Data Management Policy, and ensure that the policy, including related measures, methods, and data practices, is reviewed at least once per year or upon significant changes, as appropriate.

7.2.7 Monitor, track, and evaluate the organization's data governance implementation at least once per year, covering at a minimum:(1) Data governance readiness assessment, (2) Data quality assessment and (3) Data security assessment

7.2.8 Ensure the allocation of sufficient budget, human resources, and technology resources to support effective data management.

7.2.9 Other requirements as additionally specified by the organization.

7.3 Data Quality

7.3.1 Establish a Data Quality Management Policy to serve as a framework for ensuring that organizational data meets defined quality criteria, including:

(1) Accuracy
(2) Completeness
(3) Consistency
(4) Timeliness
(5) Relevance
(6) Availability

Data custodians are responsible for managing and overseeing data quality to build confidence among data users, while data users are encouraged to provide feedback to data custodians to continuously improve data quality.

7.3.2 Establish measurable data quality criteria and develop data quality improvement plans that define quality indicators and action plans to effectively manage data quality. Data collection processes shall be designed to support quality evaluation in alignment with such criteria and embedded into information systems and business processes (Quality by Design) to reduce errors and improve quality from data entry or data creation through data processing.

7.3.3 Regularly assess and manage data quality throughout the data lifecycle. Data owners and data custodians should define data quality frameworks specific to data categories or domains, such as the Quality Assurance Framework of the European Statistical System (ESS QAF), which may be used as a reference.

7.3.4 Develop processes or mechanisms that allow users to provide feedback or report issues to data owners, particularly for critical data such as Master Data and Reference Data.

7.3.5 Other guidelines as additionally defined by the organization.

7.4 Data Classification and Data Confidentiality Levels

7.4.1 Define data classification categories and confidentiality levels applicable to all forms of organizational data, including paper-based documents and digital data, by assessing the impact of data to determine appropriate classification levels. Appropriate security levels shall be defined for data creation, storage, usage, and access. These classifications shall apply to personnel and authorized third parties, and roles and responsibilities for data classification shall be clearly assigned to ensure proper protection, management, and governance of data.

7.4.2 Datasets shall be labeled in accordance with assessment results and assigned appropriate classification and confidentiality levels, including backup classification labels (if applicable), such as:

Classification Level	Definition
blic	Information that may be disclosed to external parties without restriction or formal request.
Internal Use	Information not freely disclosed by the organization, typically private in nature (personal or organizational). Unauthorized disclosure is undesirable, even if the impact may not be severe.
Confidential	Sensitive information that may cause loss, embarrassment, legal consequences, or damage to the interests of the data owner if disclosed to unauthorized persons or organizations.
Secret	Highly sensitive information that may result in serious loss, reputational damage, financial or asset loss, or significant impact on organizational or national interests if improperly disclosed or lost.
Top Secret	Extremely sensitive or restricted information. Unauthorized disclosure may result in the most severe damage to organizational security, reputation, financial stability, or vital interests.

7.4.3 Continuously govern and monitor system usage security and data access patterns through automated processes or manual review to identify external threats, ensure proper system maintenance, and monitor environmental changes resulting from system updates or software installations.

7.5 Data Lifecycle Management

7.5.1 Establish policies, guidelines, and management environments that support secure data lifecycle management, data privacy protection, and high data quality.

7.5.2 Develop and continuously update data set management practices, including security controls aligned with data classification and confidentiality levels.

7.5.3 Store data in accordance with defined data classification standards, ensuring data accuracy, completeness, and timeliness. Access rights and appropriate systems/tools shall be defined to protect data security and quality. Data shall be disposed of in accordance with established practices and applicable laws.

7.5.4 Establish guidelines and standards for data processing and usage to ensure data is used appropriately and in accordance with intended purposes to maximize value.

7.5.5 Disclosure of data that violates laws, regulations, orders, policies, or guidelines is strictly prohibited, regardless of data format or storage location. Disclosure shall require prior authorization from the designated organizational representative or data owner. Appropriate disclosure channels shall be established to ensure ease of access and use where permitted.

7.5.6 Define processes, technologies, and technical standards for data exchange, and establish licensing agreements or data-sharing agreements governing data exchange and data usage.

7.5.7 Establish guidelines for data security, data quality, and data privacy protection, including guidance for coordinators, and ensure that data management practices comply with defined standards and guidelines.

7.5.8 Promote awareness and understanding of data lifecycle management among internal and external stakeholders.

7.6 Data Disposal

7.6.1 Responsibilities of the Data Owner

7.6.1.1 Ensure that critical data or personal data is securely destroyed on devices prior to device disposal.

7.6.1.2 Apply appropriate measures or techniques to delete or overwrite critical or personal data stored on devices before allowing reuse, to prevent unauthorized data access.

7.6.1.3 When destruction of critical or personal data stored in the media is required, the following methods shall be applied to prevent data recovery:

- Flash Drives: Physically destroyed by crushing or shredding
- Paper Documents: Shred using document shredders
- CD/DVD Media: Shred using CD/DVD shredders, drill holes, or physically destroy
- Hard Disk Drives (HDD): Crush, shred, drill, or securely erase data using formatting or multiple overwrite methods
- Solid-State Drives (SSD): Securely erase data using formatting or multiple overwrite methods

The organization may engage an external service provider to destroy data storage media. Media must be securely stored in locked locations, and destruction shall be performed on-site under supervision of organizational personnel throughout the process. Records of destruction shall be retained as evidence. Data destruction shall be conducted once per year during January–February.