TURNKEY COMMUNICATION SERVICES PUBLIC COMPANY LIMITED

Information Technology Policy

P-EXC-014

Information Technology Policy

Objectives

To establish guidelines for the control, security, and use of information technology within Turnkey Communication Services Public Company Limited ("the Company"), ensuring efficient utilization in accordance with security standards and compliance with the Computer-Related Crime Act B.E. 2550 (2007) and its amendments.

Scope

This policy defines the rules, regulations, standards, operational procedures, and security measures covering all information technology–related operations for both system administrators and users. It consists of:

Part 1: Information Technology Control and Management - Serving as regulations and operating procedures for employees in the Information Technology Department.

Part 2: Information Technology Usage - Serving as guidelines for the use of information technology by all employees.

Part 1: Information Technology Control and Management

To ensure that the Company's information technology systems operate efficiently, securely, and continuously in support of all employees, as well as to prevent potential threats or cyber risks, the Company has established IT control and management measures as standards and guidelines for all employees in the Information Technology Department. These include:

- Assignment of responsibilities
- Control of access to the computer data center
- Control of access to information and communication technology systems
- Information technology security
- Control of information system development
- Backup of information systems
- Emergency and incident response
- Problem resolution and reporting

Assignment of Responsibilities

Objectives

To establish guidelines for appointing system administrators and assigning responsibilities related to the access and control of the Company's information technology systems in a systematic, transparent manner, and in alignment with relevant policies.

Operating Guidelines

1. Appointment of System Administrators - The Head of the Information Technology Division shall evaluate and nominate system administrators, with clearly defined duties and responsibilities.
2. Executive Approval - All appointments and assigned responsibilities must be approved by authorized executives to ensure that roles are appropriate and auditable.
3. Preparation and Review of Job Descriptions - Job descriptions for IT personnel shall be prepared and regularly updated to reflect current organizational structure and evolving technologies.
4. Clear Communication of Roles - Individuals assigned system administration duties must be clearly informed of their responsibilities, scope of work, and system access rights by the division head.
5. Actions Beyond Assigned Authorization - In necessary situations—such as urgent problem resolution or remote access—prior approval must be obtained, and a summary report of actions taken must be submitted to the responsible administrator.
6. Use of External Service Providers - When outsourcing technology management or support services is required, the Company shall assess the provider's qualifications, reliability, and security practices before engagement.

Control of Access to the Computer Data Center

Objectives

To ensure appropriate control of access to the computer data center by limiting entry to authorized personnel only, thereby reducing the risk of loss or damage to the organization's information technology infrastructure.

Operating Guidelines

1. Access Control System - The computer data center shall be equipped with an access control system, such as electronic key cards, fingerprint scanners, or other appropriate authentication technologies. The system must be capable of recording entry and exit logs.
2. Access Authorization - Access rights shall be granted only to personnel who have direct responsibilities related to operations within the area, and such access must be approved by the relevant authorized personnel.

3. Access Information Management - Information related to authorized individuals—such as names, card numbers, or authentication methods—shall be properly maintained and securely stored in accordance with applicable security standards.
4. Periodic Log Review - Entry and exit logs of the computer data center shall be reviewed periodically to detect irregular or unauthorized activities in a timely manner.
5. Access for External Personnel - When external parties require access to the computer data center—for activities such as installation or maintenance—prior approval must be obtained. The request shall specify details such as the purpose, duration, and coordinator. Access must be monitored and controlled by assigned personnel.

Control of Access to Information and Communication Technology Systems

Objectives

To establish controls over access to information technology systems, including the addition, modification, and updating of system components, in order to ensure accurate operations, proper oversight, and prevention of adverse impacts on the Company's information technology systems.

Operating Guidelines

1. User Account Creation and Management - The creation and management of user accounts shall follow an approved process authorized by the relevant authority and must align with the user's assigned roles and responsibilities.
2. Termination or Deactivation of User Accounts - User accounts shall be suspended or deactivated within an appropriate timeframe when no longer required, and records of such actions must be properly documented and retained.
3. Control of Access to Computer Systems - Access to computer systems shall be restricted to individuals who are officially assigned or authorized. Users shall not transfer or share access rights with others without authorization.
4. Control of Access to Database Systems - Access to database systems shall be limited to clearly designated personnel, supported by documented approval records that can be audited when necessary.
5. Control of Access to Network Equipment - Access to or modification of network equipment shall be governed by authorized personnel, and all changes must be properly logged and documented.
6. Control of Access by External Parties - Permission for external individuals to access systems or controlled areas shall follow a prior approval process, and their activities must be closely supervised.
7. Remote Access Control - Remote access to Company systems shall be conducted only through secure channels, such as an approved VPN, with appropriate time restrictions and regular monitoring of usage.

Information Technology Security

Objectives

To ensure that the Company's information technology systems operate efficiently, remain secure, and provide continuous service, while preventing issues arising from improper system usage and protecting against various cyber threats.

Operating Guidelines

1. Physical and Environmental Security - Controlled areas housing IT systems must maintain proper temperature, humidity, fire protection, and equipment maintenance to ensure safe and efficient system operations.
2. Computer System Security - The assignment of access rights and password usage must be systematically controlled, aligned with user responsibilities, and adaptable to emergency situations.
3. Network System Security - The installation, modification, or access to network systems must be authorized and managed through secure, auditable processes.
4. Database Security and Batch Job Control - Batch job operations must be properly controlled, monitored, and reported to prevent errors that could impact database integrity.
5. Intrusion Prevention - Antivirus or anti-malware systems must support automatic updates and be routinely monitored to ensure readiness and protection against threats.
6. Software Management - Software usage must comply with legal licensing requirements. System updates or upgrades must be preceded by proper data backup, and all changes must be appropriately documented.
7. Password Policy - Passwords must meet complexity requirements, be changed periodically, and be managed to prevent unauthorized access.
8. Internet Usage Logging - The organization must maintain a system to log and review internal users' internet activity, providing traceable information when necessary.

Control of Information System Development

Objectives

To establish processes for the development and enhancement of the Company's information systems, as well as control measures to ensure that the resulting systems meet their intended objectives, operate accurately and completely, and remain fully auditable.

Operating Guidelines

1. Initiation of System Development and Enhancement - Development or improvement activities must begin with a clearly separated working environment and be based on a requirements analysis approved by the authorized personnel.
2. Internal System Development - Internal development must follow the System Development Life Cycle (SDLC), including the preparation of supporting documentation, testing within a separate environment, and obtaining formal approval prior to production deployment.

3. Software Acquisition – The procurement of software must consider suitability and cost-effectiveness, supported by documentation detailing required functionalities and budget proposals for approval.
4. Development by External Parties - When outsourcing system development, clear requirement specifications must be prepared, and the vendor must undergo evaluation and quality control processes according to established procedures.
5. Control of External Developers - External developers must deliver complete documentation and test results. System deployment to the production environment must undergo joint verification and approval.
6. Special Case Production Deployment - Any installation or direct access to the production system by external parties requires prior authorization and must be formally logged.
7. Data Conversion Control - Data migration must be validated both before and after conversion to ensure that data in the new system matches the original source and is fully auditable.
8. System Acceptance Testing - System testing shall follow an approved test plan, with results certified jointly by relevant users. Version records must be documented, and final approval must be obtained before going live.

Information System Data Backup

Objectives

To establish guidelines for backing up and restoring information system data in a secure, reliable manner, ensuring availability and continuity in the event of unexpected incidents.

Operating Guidelines

1. Development of Backup Procedures - Backup and restoration manuals should be created and regularly updated, covering all critical systems.
2. Daily Data Backup - Backup operations shall follow a clearly defined plan and be performed automatically or semi-automatically to ensure consistency and continuity.
3. Backup Verification - Each backup process must be reviewed, with results recorded and any issues reported to the authorized personnel.
4. Backup Data Storage - Backup data should be stored both physically and in cloud formats, including off-site storage locations to ensure resilience in unforeseen situations.
5. Transfer of Backup Data - The movement of backup data must be controlled through logging systems and a sign-in/sign-out process that allows for auditability.
6. Data Restoration Testing - Data restoration must be tested at scheduled intervals, and results documented to verify the readiness of the backup system.
7. User-Initiated Data Restoration - Data restoration requests submitted by users must undergo formal approval and be carried out under the supervision of the responsible department.

8. Handling Restoration Issues - If problems occur during data restoration, authorized personnel must be notified immediately, and contingency plans activated to manage the emergency situation.

Emergency Response and System Recovery

Objectives

To establish guidelines for restoring the Company's information technology systems so they can resume normal operations as quickly as possible in the event of an emergency that causes system disruption.

Operating Guidelines

1. Preparation of Critical Information for Emergency Response - Important IT-related information—such as network diagrams, equipment inventories, and system architecture documents—should be prepared and maintained for use during system recovery in unexpected situations.
2. Recovery of Core Systems (e.g., ERP System) - When a core system becomes unavailable, relevant personnel must be contacted immediately to collaborate on a recovery plan. Restoration must follow established procedures under authorized supervision.
3. Data Restoration Using Backup Data (Core Systems) - Data restoration must be approved beforehand. The integrity of the backup data must be verified, and all actions coordinated with relevant teams to ensure safe and proper restoration.
4. Post-Recovery Reporting - A detailed report should be prepared after system recovery, summarizing the incident, root cause, corrective actions taken, downtime duration, and preventive measures to avoid recurrence.
5. Recovery of Other Systems (Non-ERP Applications) - When other applications become unavailable, initial assessments should be performed promptly, and corrective actions should be taken in coordination with the responsible system administrators or developers.
6. Data Restoration for Other Systems - Before restoring data from other systems, approval must be obtained, the accuracy of the backup data must be verified, and restoration must be carried out according to a secure and approved plan.
7. Incident Reporting for Other Systems - Once the system has been restored, an incident report—aligned with the reporting format used for core systems—should be prepared for reference and for improving future emergency response plans.

Problem Resolution and Reporting

Objectives

To establish systematic, transparent, and auditable procedures for receiving issues, resolving problems, and reporting outcomes.

Operating Guidelines

1. Issue Intake and Initial Handling - IT personnel are responsible for receiving issue reports, conducting an initial assessment, and resolving the problem within their scope of responsibility, or escalating the issue to the relevant specialists when necessary.
2. Coordination and Consultation - If the issue cannot be resolved within the department, coordination should be made with supervisors or relevant experts. External service providers may be engaged when required.
3. Recordkeeping and Reporting - Records of reported issues, resolution methods, and work outcomes must be systematically maintained. A summary report should be prepared and submitted to the authorized personnel on a monthly basis.
4. Severe Impact Cases - If an issue significantly affects organizational operations, it must be reported to senior management immediately.
5. Root Cause Analysis and Recurrence Prevention - Recurring issues should undergo root cause analysis to identify systemic problems and develop preventive measures and long-term process improvements.
6. Urgent Cases or Deviations from Standard Procedures - When urgent corrective action is required and normal procedures cannot be followed, temporary approval may be obtained, with supporting documentation completed as soon as possible thereafter.

Part 2: Information Technology Usage Policy

This section serves as the guideline for all employees of the Company in the use of information technology. It includes the following areas:

- Control of Information Technology Usage
- Use of Computers
- Use of Computer Networks and User Accounts
- Use of Electronic Mail (E-mail)
- Use of the Internet
- Data Maintenance on Computers
- Computer Virus Protection
- Use of Artificial Intelligence (AI) within the Organization

Control of Information Technology Usage

Objectives

To ensure that employees understand the proper use of the information technology resources provided by the Company.

Operating Guidelines

The objectives, scope, and methods for using information technology shall be clearly defined to ensure correct and efficient usage in compliance with legal requirements and the Company's security standards, and communicated to all employees.

1. Appropriate Use of IT Resources - Employees should use the Company's computer systems and networks solely to support work-related activities and avoid the use of IT resources for non-organizational purposes.
2. Use of Personal Devices - If personal devices must be used in conjunction with the Company's systems, employees should inform and seek guidance from the responsible IT personnel.
3. Compliance with IT Usage Guidelines - Users must be aware of and comply with the Company's information technology usage guidelines and adhere to all data security requirements.
4. Guidance for External Personnel - External parties working within the organization must receive appropriate instructions regarding the use of the Company's IT systems.
5. Monitoring of IT System Usage - The Company may monitor IT system usage as necessary if actions that could impact security or operational efficiency are suspected.
6. IT Support Channels - The Company should provide channels for contacting system administrators to obtain assistance or guidance regarding system usage.

Use of Computers

Objectives

To ensure that employees understand the allocation and proper use of computers provided by the Company.

Operating Guidelines

1. Computer Allocation - Computers shall be allocated to employees based on the suitability of their job responsibilities and upon approval by the relevant authorized personnel.
2. Use of Personal Computers or Storage Devices - Employees should not use personal computers or portable storage devices within the organization unless explicit permission has been granted.
3. Appropriate Use of Company Computers - Company computers must be used solely to support organizational tasks. Employees should not store or use inappropriate, illegal, or copyright-infringing programs or content.
4. Legal Responsibility - If a computer is used in a manner that leads to legal consequences, the user shall be responsible in accordance with applicable laws.
5. Unauthorized Software Installation - Employees must not modify or install operating systems or licensed software without prior approval.
6. Unauthorized Hardware Modifications - Additional hardware installation or modification must not be performed without the approval of the relevant personnel.
7. Proper Care of Computers - Employees must maintain their assigned computers in good working condition. In cases where damage occurs due to improper use, the Company may require the user to share responsibility as deemed appropriate.

Use of the Computer Network and User Accounts

Objectives

To allocate user accounts appropriately, enabling employees to access the Company's computer network systems according to their respective job responsibilities.

Operating Guidelines

1. Confidentiality of User Accounts - Employees must keep their user accounts and passwords confidential and should change their passwords regularly.
2. Prohibition of Shared Accounts - User accounts must not be shared, and passwords must not be disclosed to others.
3. Use of ERP and Other Systems - The use of ERP and other systems must comply with the guidelines established by the Company.
4. Opening or Closing User Accounts - Requests to create or deactivate user accounts must be submitted through the designated channels or reported to the responsible personnel.
5. Proper Use of Authorized Access - Employees granted access rights must use systems with caution and safeguard their access credentials responsibly.

6. Network Management - The organization is responsible for managing, controlling, and allocating network resources based on job requirements and suitable operating environments.
7. Restriction on External Access - Employees must avoid allowing external individuals to access the Company's network without authorization and must not install personal networking equipment within Company premises.
8. Unauthorized Network Configuration Changes - Employees must not modify commands or data on network equipment unless officially assigned or authorized.
9. Avoiding Disruption to Network Operations - Employees should refrain from any activities that could cause network malfunction or service disruption.
10. External Access Authorization - When external personnel require network access for work purposes, prior approval must be obtained, and appropriate access logs must be maintained.

Use of Electronic Mail

Objectives

To ensure that employees use the Company's electronic mail system efficiently and appropriately.

Operating Guidelines

1. Purpose of Email Use - The Company's email system is provided solely for work-related and organizational purposes.
2. Opening or Closing Email Accounts - Requests to create or deactivate email accounts must be submitted through the forms or channels designated by the Company and approved by authorized personnel.
3. Proper Communication Etiquette - Employees should use polite and professional language and avoid sending incorrect, harmful, or misleading information that may negatively affect others.
4. Prohibited Content - It is strictly prohibited to send inappropriate content, including messages or images of obscene or unethical nature.
5. Compliance with Laws - Email communications must comply with applicable laws such as the Computer-Related Crime Act.
6. Sender Identification - Emails should not be sent anonymously; the sender's identity must be clearly indicated.
7. Email and Attachment Size Limits - Employees should limit email size, including attachments, to no more than 20 MB to ensure optimal system performance.
8. Handling Large Files - If employees need to regularly send files larger than 20 MB, they must request approval or use services provided through designated Company channels.

Use of the Internet

Objectives

To ensure that employees can use the Company's internet services efficiently and safely, while adhering to applicable laws and appropriate ethical standards.

Operating Guidelines

1. Work-Related Internet Use - The internet provided by the Company is intended to support work-related tasks, information research, and the development of employee skills within the context of their duties.
2. Compliance with Laws and Ethics - Internet usage must comply with applicable laws, including the Computer-Related Crime Act (No. 2) B.E. 2560 (2017), and must not involve activities that violate moral standards or negatively impact others.
3. Identity and Security Practices - Employees should access the internet using the user accounts provided by the Company, keep passwords secure, and strictly adhere to the Company's network usage guidelines.
4. Appropriate Use of Organizational Resources - Employees should avoid using Company email addresses to register for services or websites unrelated to work, in order to prevent privacy risks or exposure to external threats.
5. Internet Usage Logging - The Company may record internet usage history for security purposes and for retrospective review as permitted by law.
6. Connection of External Devices - Connecting personal devices or any non-authorized equipment to the Company's internet network requires prior review and approval by authorized personnel to maintain overall system security.

Data Management on Computers

Objectives

To promote safe, organized, and systematic data storage, backup, and usage practices, while minimizing the risk of important data being lost or leaked.

Operating Guidelines

1. Caution in Information Disclosure - Internal organizational data must be used and disclosed with appropriate discretion and authorization. When information must be shared with external parties, employees must follow established procedures and the approval hierarchy of their respective departments.
2. Use of Shared Storage (Share Drive) - The Company may provide centralized shared storage (Share Drive) for each department. Users may request additional space through the Company's standard request form.
3. Storage Management - Users should organize data efficiently and manage shared storage space responsibly. Personal files or non-work-related data should not be stored in shared or public folders.
4. Data Backup - Employees are encouraged to regularly back up important data, whether on internal device storage (Drive C:/D:) or on secure storage media such as the Share Drive or approved external backup devices. Cross-drive backup methods are recommended to reduce the risk of hardware-related data loss.

5. Organizational Backup Systems - The Company's servers may automatically perform scheduled backups to enhance the security and reliability of shared data.
6. Device Security - Portable computers provided by the Company (e.g., notebooks) may be preconfigured with security features to prevent unauthorized access. Employees should avoid altering these security configurations.
7. Management of Confidential and Critical Files - Confidential files—such as those related to accounting, finance, or business strategy—must be encrypted and clearly labeled as confidential to ensure strict handling and restricted access.
8. Use of Portable Devices and Data Transfer - When data must be taken offsite using portable media (e.g., USB drives), files should be encrypted prior to transfer. Employees should use only Company-recommended software to ensure data security.
9. Control of Data Export Outside the System - Transferring data via portable storage devices, cloud services, or social media must follow the Company's approval process and policies to prevent accidental leakage.
10. Use of Personal Portable Devices in the Company Network - When personal portable devices must be connected to Company computers, employees must notify and obtain approval from the system administrator or responsible supervisor. Usage may be restricted to a limited period (e.g., 90 days), after which the system may automatically revoke access rights.

Computer Virus Protection

Objectives

To ensure continuous and secure use of the Company's information technology systems while minimizing the risk of damage to data, applications, and equipment caused by cyber threats such as viruses, malware, or attacks from unsafe sources.

Operating Guidelines

1. Organization's Antivirus System - The antivirus system deployed within the Company is configured to automatically update virus definitions through the network each time the computer is turned on. Users should allow the antivirus software to operate normally to ensure continuous and effective protection.
2. Data Storage Practices - Employees are encouraged to store important data on Drive D:, which is separated from the operating system on Drive C:, to reduce the risk of data loss should a system attack or virus infiltration occur.
3. Avoiding High-Risk Websites - Users should avoid accessing websites that may pose security risks, such as pornographic sites, gambling sites, uncertified gaming platforms, or illegal websites, to prevent exposure to malware and other threats.
4. Caution When Downloading Files - Users should carefully review any prompts to download files or open links from unknown or untrusted sources to avoid downloading files that may contain malware or viruses.
5. Handling Non-Company Devices - When it is necessary to perform actions involving non-company-owned devices—such as formatting, connecting external equipment, or other operations—users must seek guidance or obtain approval from the system administrator or relevant supervisors to ensure overall IT security.

Use of Artificial Intelligence (AI) Within the Organization

Objectives

To establish guidelines for the responsible, transparent, and ethical use of Artificial Intelligence (AI) within the organization, ensuring compliance with relevant laws, minimizing potential risks, and fostering trust among employees, customers, and stakeholders.

Operating Guidelines

1. Scope of AI Usage - This guideline applies to all personnel at every level, as well as authorized external parties who use AI within the organization's systems. It covers AI software, platforms, and services—whether developed internally or sourced from external providers.
2. Respect for Privacy - AI usage must not infringe upon personal privacy or cause negative impacts to the organization or any individual, whether intentional or unintentional.
3. Critical Decision-Making - AI must not be used as the sole decision-maker in high-impact matters—such as personnel selection or contract approvals—without prior review and verification by responsible decision-makers.
4. Transparent Use of AI - AI must not be used to manipulate information, generate false data, or create misleading impressions under any circumstances.
5. Protection of Data and Confidential Information - Users must avoid disclosing internal information, proprietary algorithms, AI system mechanisms, or any confidential data belonging to the organization or external parties.
6. Verification Before Deployment - AI systems must undergo accuracy, security, and bias testing before being deployed, especially in activities involving critical decisions or sensitive information.
7. Personal Data Protection (PDPA) - Any AI usage that involves personal data must be based on the data subject's consent and must fully comply with personal data protection laws.
8. Knowledge and Training - AI developers and users should receive regular training or guidance on AI ethics, best practices, and AI-related risks.
9. Reporting Channels - The organization must provide clear channels for employees and customers to express concerns, feedback, or complaints regarding AI usage.
10. AI System Maintenance and Improvement - AI systems must be continuously reviewed and updated to remain current, reduce risks, and improve performance.
11. Access Rights and Authorization Control - Access to the organization's AI systems must not be transferred or shared with unauthorized external parties. Users must exercise caution, and in cases where improper use leads to damage, responsible individuals may be held accountable as appropriate.

This Information Technology Policy was approved by the Executive Committee Meeting No. 11/2025 on November 3, 2025, and has been effective on November 3, 2025.

- Sayam Tiewtranon -

(MR. SAYAM TIEWTRANON)
Managing Director / Chairman of the Executive Committee