710/2568

25 November 2025

Saksiam Leasing Public Company Limited

Information Systems and Data Communication Network Usage Policy

To ensure that the Information Systems and Data Communication Network Usage Policy of the Company is comprehensive and more suitable for operational requirements, the Announcement regarding the Information Systems and Data Communication Network Usage Policy No. 884/2567, dated December 27, 2024, is hereby revoked and replaced by this Announcement.

1. Objectives

1.1 To serve as a guideline for operational security relating to access control and the usage of the Company's information systems.

1.2 To ensure that responsible persons and relevant stakeholders—including executives, users, system administrators, and external personnel working for the Company—are aware of the guidelines for securing the Company's information systems, recognize their importance, and strictly cooperate in complying with the designated guidelines.

2. Responsible Parties

The Managing Director, Deputy Managing Director, Information Technology Department Manager, and personnel appointed and assigned by the Company to oversee the Company's information systems.

3. Definitions

The definitions in the following topics are provided by the Company to establish a mutual understanding within this policy document, with details as follows:

3.1 **Information Systems:** Interrelated components that work together to collect, record, process, store, and distribute information to support decision-making and managerial functions, including planning, organizing, coordinating, controlling, and internal communication. This includes information systems related to customer service, various administrative operations, and information management systems used in the Company's business (details as per the attached document).

3.2 **Data Communication Network:** The network system responsible for connecting data between the Head Office, branches, and Company units, covering connections through the Company's Internet, Intranet, and Wireless Local Area Network (Wireless LAN).

3.3 **Server:** A computer designed to provide information system services for the Company, such as Web Servers, Database Servers, Mail Servers, File Servers, Application Servers, Virtual Servers, and Hyper-Converged Infrastructure (HCI), among others.

3.4 **Network Equipment:** Devices responsible for transmitting data between servers, computers, and peripheral devices within the data communication network. Network equipment consists of Routers, Network Switches, Load Balancers, Firewalls, Wi-Fi Access Points, Wi-Fi Controllers, and Cables.

3.5 **Computer:** Computers for users in various forms, consisting of a CPU, Mainboard, Memory, Hard Disk, Power Supply Unit (PSU), Monitor, Mouse, Keyboard, including Uninterruptible Power Supplies (UPS) or backup batteries, as well as other components as follows:

3.5.1 *Desktop:* A computer designed for permanent use on a desk, not intended for modification or easy mobility.

3.5.2 *Laptop:* A portable computer that integrates a screen, keyboard, and processing unit into a single, small-sized design.

3.5.3 *Tablet:* A portable computer with a touchscreen used instead of a mouse and keyboard, featuring a built-in processing unit, memory, and battery.

3.6 **Operating System (OS):** Software responsible for managing various resources on a computer or server and managing the user interface. Examples of operating systems include Microsoft Windows, Linux, FreeBSD, Android, and iOS.

3.7 **Application Software:** Programs installed on a computer or programs that run via web browsers, which are off-the-shelf software or programs developed for operational utility. Examples of application software include Microsoft Office, Google Workspace, Google Drive, LINE, etc.

3.8 **Database Management System (DBMS):** Software that controls and manages data within a database. Examples of database management systems include:

- NoSQL Databases: e.g., MongoDB
- Relational Databases: e.g., MySQL, MariaDB, MSSQL, Oracle Database, Sybase

3.9 **Peripherals:** Devices used to input and output data to and from a server or computer for storage or printing purposes. Examples include a mouse, keyboard, image scanner, laser printer, inkjet printer, dot-matrix printer, fingerprint scanner, barcode scanner, USB drive, Smart Card Reader (Thai National ID Card Reader), etc.

3.10 **System Administrator (Sysadmin):** A person responsible for overseeing the operation of information systems, user registration, data backup, data recovery, troubleshooting potential operational issues, monitoring and auditing system and data security, and coordinating with system developers to ensure that information systems can serve users efficiently.

4. Access Control

Access control and the definition of usage rights for information systems, including the modification of the Company's various systems, must comply with this policy. Since systems and data are the Company's property, any modification, improvement, or access must be assigned by the Information Technology Department Manager. The following policy is established as an operational and control guideline:

4.1 Information systems related to customer service, namely the LMIS loan system, the Hire Purchase Loan system (HPS), and the customer loan payment system (SAK Payment), are critical to the Company's business operations and contain confidential Company and customer data. The Company is required to keep this data confidential and enforces a policy requiring system access via a Username and Password based on the authorized rights of each user per system.

4.2 The Company's administrative systems, namely the Payroll system, Employee Information, the SAP accounting system, and the Head Office central file system, are subject to a policy restricting access via Username and Password to relevant users only.

4.3 The Data Modification Tool (DMT) system is used for data access. Users of this system must be authorized individuals with access rights to modify, add, or delete various data.

4.4 For other information systems, such as electronic mail (e-mail) or websites, group accounts are permitted as appropriate based on the nature of use (e.g., branches, units, or departments within the Head Office) to prevent operational bottlenecks.

5. Granting Access Rights to Information Systems

Granting access and usage rights for the Company's information systems is the responsibility of assigned individuals, categorized by operational levels as follows:

5.1 Operational/User Level (Application System) and Application-level Administrator Level: Passwords are configured as follows:

(1) Password age must not exceed 90 days (3 months).

(2) Password length must be at least 6 characters.

(3) Password complexity must include numbers and both uppercase and lowercase English letters.

(4) Maximum allowable failed login attempts must not exceed 5 times.

(5) Users are prohibited from reusing any of their last 3 previous passwords.

5.2 Operating System (OS) Level for Applications on Servers: Applications must be installed on essential operational operating systems (OS) on servers, such as CentOS and Ubuntu. Password expiration is not enforced for these systems because these underlying operating systems must interact with applications that maintain continuous connections to the main database. Authorized individuals must have

access to manage and control host computers to ensure uninterrupted operations. It has been assessed that this does not pose a security risk to system access, as authorized individuals must be specifically assigned by the Information Technology Department Manager only. However, the password configuration requirements are as follows:

(1) Password length must be at least 8 characters.

(2) Password complexity must include numbers, uppercase and lowercase English letters, and at least 1 special character (e.g., #, !, @, $, %, &, or *).

(3) Maximum allowable failed login attempts must not exceed 5 times.

(4) Users are prohibited from reusing any of their last 3 previous passwords.

5.3 Database Level and OS Level on Servers: The Company's database systems do not enforce password expiration for data access because various applications constantly connect to the database to read and write data. If the password used in these systems changes, the applications must be modified or updated every time. (It has been assessed that this does not pose a security risk to data and database security, as general users cannot access the database directly). High-privilege accounts, such as the Root account of the operating system and database system, are restricted to senior executives or specifically assigned administrators.

5.4 Access via Virtual Private Network (VPN): For remote access to connect to the Company's database and server operating systems from the outside, users must obtain authorization from the person assigned by the Information Technology Department Manager or a higher authority. Connection to the database is permitted only via a Virtual Private Network (VPN) or the internal Local Area Network (LAN), and users must login with their own Username and Password every time.

5.5 Approval Process: Permissions to access systems, job transfers/ reallocations, employment terminations, and the suspension of access to critical information systems must always be recorded and kept as evidence.

5.6 Other Systems: For other information systems, such as electronic mail or websites, group accounts are permitted as appropriate based on the nature of use (e.g., branches, units, or departments within the Head Office) to prevent operational bottlenecks.

5.7 Username Creation: Usernames must be configured in English letters (either uppercase or lowercase) matching the name on the user's National ID card. If a username already exists, it should be followed by a number or the first letter of the surname. If it still conflicts, the second letter of the surname (or subsequent letters in order) shall be added until it is unique. For regional or field units, usernames must be defined using the unit's code (e.g., SAK0100) or the English name of the Head Office department (e.g., Finance or Internal Audit).

6. Duties and Responsibilities of Executives

6.1 Clarify and inform information system users regarding policies, standards, operational frameworks, procedures, practices, guidelines, and processes of the Company regarding cyber security.

6.2 Supervise, guide, and issue warnings in the event that incorrect or inappropriate practices regarding the use of information systems and data communication networks are observed.

6.3 Consider disciplinary action against violators equally and fairly.

7. Users' Duties, Responsibilities, and Etiquette

7.1 Users of information systems must learn, understand, and strictly comply with the Company's policies, standards, operational frameworks, procedures, practices, guidelines, and processes regarding the use of information systems and relevant communication networks related to cyber security.

7.2 Users have a duty to immediately change any temporary passwords received upon logging in for the first time, set a new password that is difficult to guess, maintain password confidentiality, and change the password every 90 days or when deemed necessary. Passwords and any other access codes designated by the Company to access information systems or data must be kept as the personal secret of the user. Users must prevent others from knowing them, must not share them, must not reuse old passwords, must not set passwords that can be easily guessed, and must not use identical passwords across all systems they have rights to access.

7.3 Data duplication or copying must comply with the Company's cyber security regulations and requirements.

7.4 Users have a duty to learn how to use computers and peripheral devices correctly, and help maintain the equipment they use regularly or are assigned to care for so that it functions normally (e.g., cleaning, observing signals or warning lights, and noticing abnormal operations). Users should regularly check the operation of the hard disk and file system at least every 6 months.

7.5 Users must not uninstall, disable, or modify software/programs installed by system administrators, particularly antivirus and anti-malware programs, as this causes risks that can prevent computers from working normally. If unsure, users must consult a system administrator first.

7.6 Users must not download uncertified or unlicensed software/programs, or software that carries risks of viruses and malware, onto their assigned computers. Users should exercise caution when accessing websites on the Internet and must not guess and click buttons displayed on the screen.

7.7 Users must not use Company computers to browse websites that are unrelated to work, morally prohibited, against public order, illegal, or pose virus and malware risks,

such as online gambling, online games, watching movies or pornographic images, or downloading files from unknown sources.

7.8 During working hours, users must not use the Company's devices and communication networks to view or download large multimedia files, such as watching clips, movies, listening to music, or watching sports broadcasts, which do not benefit operations. This represents an inappropriate use of network resources and may impact the work performance of colleagues.

7.9 Users must not store personal files, such as music, pictures, or clips that do not benefit operations, on Company computers.

7.10 Users must not store, play sound, or display images that are contrary to morality, illegal, pornographic, or media that may cause discomfort to colleagues, such as political opinions or religious beliefs/doctrines.

7.11 Users must not use computers, printers, copiers, faxes, and information equipment belonging to the Company— especially consumables— for personal matters, and should use personal items for such purposes.

7.12 Users must ensure that computers receive power from a UPS and verify that the UPS can still back up power during brownouts or power drops (UPS batteries have an average lifespan of 1.5–2 years). When a UPS fails to work, the battery or the UPS unit must be replaced immediately, as it poses a risk of damaging hard disks and stored data beyond recovery.

7.13 If used computers or peripherals encounter problems, users must consult a system administrator or return the item to the Head Office to requisition a replacement. Users should not attempt unauthorized repairs, as this often fails to resolve the problem completely, resulting in wasted money and time.

7.14 Users must log out or log off from all systems when not in use for an extended period and turn off computers and other peripherals immediately after working hours.

7.15 Users must apply a password-protected Lock Screen when leaving their computers unattended or performing other short-term activities to prevent unauthorized access by other individuals.

7.16 Fully cooperate with the Company in protecting its information systems and data communication networks by notifying the Company immediately upon witnessing incorrect or inappropriate practices, or if any intrusion, theft, destruction, operational interference, or actions that may cause damage to the Company are detected.

8. Duties and Responsibilities of System Administrators

8.1 The Company has a duty to procure computers, network equipment, and peripherals with appropriate specifications for employees, and is responsible for installing operating systems, software, and applications ready for use. This includes repairing, procuring spare parts, and providing operational and maintenance advice to users.

8.2 System administrators have the duty to control user access rights to information systems based on roles, responsibilities, and necessity. Access rights include:
(1) Read Only,
(2) Create,
(3) Modify,
(4) Approve, and
(5) No Access.

8.3 User access to information systems must comply with policies set by the Company or be authorized by the Managing Director, Deputy Managing Director, or Information Technology Department Manager. User rights in critical systems, including the LMIS loan system, HPS loan system, and SAP accounting system, must be reviewed at least once a year.

8.4 Every information system must have designated system administration duties assigned to a System Administrator, with a clearly defined scope of duties.

8.5 System Administrator duties must include at least the following matters:
8.5.1 Maintain the user directory and account registry.
8.5.2 Set or change passwords.
8.5.3 Secure access and system usage in accordance with Company policies.
8.5.4 Perform data backups and test system data restoration within designated schedules.
8.5.5 Regularly monitor system operating conditions.
8.5.6 Troubleshoot and resolve issues to ensure information systems function normally.
8.5.7 Provide technical advice and consultation to users.
8.5.8 Supervise and monitor external parties involved in using information systems.

9. Network Communication System Usage

9.1 Network equipment, servers, computers, and every peripheral device on the Head Office communication network must be assigned a static IP Address, and an IP address registry must be maintained for auditing purposes.

9.2 Firewalls must be enabled, and port opening must be controlled. The policy mandates opening ports only as strictly necessary, and an open-port registry must be maintained.

9.3 Employees are strictly prohibited from installing network equipment arbitrarily. The installation of network equipment, such as Routers, Wi-Fi Routers, Access Points, and Switches in the Head Office, must obtain prior permission from the system administrator to prevent damage and potential interference with the network system's operations.

10. Secrecy of Data

10.1 Employees are strictly prohibited from disclosing, disseminating to unrelated individuals, or copying and moving confidential data within the Company' s information systems to external environments.

10.2 Confidential data consists of:

(1) Accounting records and reports
(2) Financial records and reports
(3) Budgets
(4) Employee profiles and income data
(5) Policies or orders not yet authorized for dissemination
(6) Strategies and business plans
(7) Personal data and loan histories of customers, as well as data linked to the aforementioned items, such as analytical data.

10.3 For the exchange of confidential data, authors and data owners must store it in private areas only. If it is necessary to exchange confidential data through electronic methods, the data owner must encrypt the data file to prevent unauthorized reading, notify the recipient of the decryption password separately, and delete the file from the exchange area once received. This must align with the Company's Personal Data Protection policy and procedures.

11. Server Room and Equipment Installation

11.1 Servers and network equipment that constitute the Company's information systems must be installed in the Server Room or designated specific locations, with access restricted to relevant authorized personnel only.

11.2 Entering the server room for operational purposes must be recorded in a logbook every time, detailing the name, entry-exit times, purpose of entry, and signature. External parties must always have the joint signature of the Company's supervisor present.

11.3 The Server Room must control temperature, humidity, and dust levels appropriately at all times, and a warning system should be provided to alert on abnormalities.

11.4 Servers and network equipment must be installed and arranged in equipment racks. Cabling must be organized neatly, and labels and diagrams showing cabling layouts and network equipment connections must be prepared.

11.5 Labels must be attached to identify servers, network equipment, and cables, alongside the consideration of using different colored cables to prevent incorrect cable connections.

12. Fault Tolerance

12.1 Information system servers must be installed with at least 2 hard disks and configured for data redundancy in at least RAID 1, 5, 6, 10, or equivalent/better configurations to prevent data damage if any single hard disk fails suddenly.

12.2 Information system servers should have at least 2 units operating concurrently in an Active/Active or Active/Standby manner, or backup servers must be provided so that they can be used interchangeably within 2 hours.

12.3 Information system servers should be installed with 2 sets of Power Supply Units (PSU) powered by 2 separate Uninterruptible Power Supplies (UPS).

12.4 Servers and network equipment must receive power only from a UPS to prevent operational disruption during brownouts or power outages, and to protect hard disks and file systems from potential damage caused by such incidents.

12.5 The information system UPS should be able to back up power for no less than 30 minutes to allow system administrators sufficient time to perform a structured system shutdown, preventing data loss and damage to hard disks, file systems, or databases.

12.6 Servers must be configured to shutdown automatically if they detect that power has been supplied from the UPS battery for longer than 30 minutes.

12.7 A backup Generator must be provided to automatically supply power to devices and temperature control systems in the server room within 5 minutes when the main power supply fails, providing continuous and adequate power until normal supply resumes.

12.8 A backup channel for Internet connection must be provided in case the primary channel becomes unavailable.

13. Backup and Recovery

13.1 Information systems where data is added, changed, or modified daily must undergo daily system data backups (details as per the attached document).

13.2 Information systems where data is added, changed, or modified weekly or monthly must undergo backups according to those periods. Systems under this scope include:

(1) Payroll and Human Resources systems.

(2) Website data dissemination systems, etc.

13.3 Data from information systems that must be backed up includes User Data, Configuration Files, and other user-related data. Backed-up data must be stored separately from the operational server currently in use.

13.4 In the event that any information system fails suddenly, a backup system or method must be available to restore operations within 4 hours.

13.5 Data backup and recovery from operational information systems must be reviewed and tested in accordance with the above policy at least once a year.

14. Logging

Login histories and usage histories in critical systems, including the modification, addition, or deletion of data, must be recorded and maintained in accordance with legal requirements.

15. Monitoring

Operational status monitoring and alerts for the network system and information system servers must be provided, allowing system administrators to check operational status and alerts remotely.

16. Documentation

16.1 User manuals, installation manuals, maintenance manuals, and backup and recovery manuals for information systems must be prepared, containing comprehensive, sufficient, and clearly understandable details necessary for system maintenance.

16.2 An information system registry must be maintained, comprising critical data for each system, including: system name, brief system services, user groups, server specifications (brand and model, CPU, memory capacity, hard disk and capacity), installed operating system, installed software, system configurations, IP Address, structural diagrams, administrator account name (passwords provided separately), administrator name and contact details, registrar name, and date of registry creation, among others.

16.3 The information system registry must be reviewed and updated according to designated periods, at least once a year.

16.4 Device specifications and user manuals for both hardware and software of information systems must be compiled and stored in electronic file formats, with at least 1 set maintained.

17. Maintenance and Spare Parts

The appropriateness of servers, computers, network equipment, peripherals, operating systems, software, and applications used in the Company must be evaluated based on performance, lifespan, suitability, maintenance costs, and spare parts availability to establish a budget for procuring replacement equipment at least once a year.

18. User Account Management Procedures in LMIS, HPS, and SAP Systems

18.1 Practices for Adding/Changing/Suspending Access Rights in LMIS and HPS Systems:

18.1.1 Adding rights for new employees:

1) The IT Department receives an instruction to add a probationary employee from the HR Department, approved by the Managing Director.
2) The IT Department correctly adds the full name, position, branch affiliation, and unit into the system.

3) The IT Department creates the username, password, usage rights, and data access permissions matching the job position.
4) The IT Manager or IT Department Head audits the addition of employee data, usage rights, and system access rights.
5) The IT Department notifies the probationary employee of their username and password on their first day of work.

18.1.2 Changing rights due to transfers or position changes:

1) The IT Department receives a position change or workplace transfer instruction from the HR Department, approved by the Managing Director.
2) The IT Department executes the change or transfer of the employee in the system according to the approved instruction.
3) The IT Department updates system access rights based on the new job position.
4) The IT Department Manager or IT Department Head audits the change, transfer, and rights configuration in the system.

18.1.3 Suspending or disabling user accounts due to resignation, suspension, or termination:

1) The IT Department receives a resignation, suspension, or termination instruction from the HR Department, approved by the Managing Director.
2) The IT Department suspends the employee's usage rights in the system.
3) The IT Department Manager or IT Department Head audits the system rights suspension.
4) The IT Department records a confirmation of rights suspension on the resignation document received from the HR Department.
5) The IT Department maintains a written control register of resigned employees.

18.1.4 Requests to change, add, or delete rights for specific menus:

1) The supervisor of the department requesting system rights adjustments must submit a memorandum requesting rights modifications for subordinates to the Managing Director or Deputy Managing Director for approval.
2) The Managing Director or Deputy Managing Director reviews and approves the rights modification.
3) The IT Department executes the rights adjustment in the operational system.
4) The IT Department Manager or IT Department Head audits the rights modification in the system.
5) The IT Department notifies the requester of the completed modification so they can access the system.

18.1.5 End-of-month summary: At the end of every month, the IT Department summarizes reports regarding the addition, modification, and suspension of usage rights in the LMIS and HPS systems, reconciling the user list in the system to match the employee data from the HR Department.

18.2 Practices for Adding/Changing/Suspending Usage Rights in the SAP System: These actions can only be performed once the Managing Director or Deputy Managing Director reviews and approves adjustments to access rights based on suitability or position, with the following practices:

18.2.1 The supervisor of the department requesting SAP access rights adjustments for subordinates must submit a memorandum requesting SAP rights modifications to the Managing Director or Deputy Managing Director for approval.

18.2.2 The Managing Director or Deputy Managing Director reviews and approves the modification.

18.2.3 The IT Department updates, modifies, or suspends rights in the SAP system.

18.2.4 The IT Manager or IT Department Head audits the rights modification in the operational system.

18.2.5 The IT Department notifies the requester of the completed modification so they can access the system.

19. Procedures for Modification, Revision, and Development of Information Systems

19.1 Information System Development Procedures according to Annual Operational Plans and Projects:

19.1.1 The IT Department prepares project plans and development details to present to the Managing Director for project approval.

19.1.2 Prepare detailed requests for approval to modify/improve systems based on the approved project plan.

19.1.3 Transmit detailed documentation to system developers to modify/improve the system.

19.1.4 System developers deploy the program onto the Development System.

19.1.5 The IT Department and users verify data within the Development System.

19.1.6 The IT Department confirms program accuracy and instructs system developers to deploy the program onto the Production System.

19.1.7 The IT Department monitors and evaluates modifications after updates are deployed.

19.2 System Modification Procedures based on Policies or Departmental Meeting Resolutions:

19.2.1 The IT Department is notified to modify, change, or develop systems based on meeting resolutions from various departments.

19.2.2 The IT Department requests program modification approval from the Managing Director or Deputy Managing Director.

19.2.3 The IT Department instructs system developers to modify the program.

19.2.4 System developers deploy the program onto the Development System.

19.2.5 The IT Department and users verify data within the Development System.

19.2.6 The IT Department confirms program accuracy and instructs system developers to deploy the program onto the Production System.

19.2.7 The IT Department monitors and evaluates modifications after updates are deployed.

19.3 The IT Department maintains a control registry for the modification and development of operational program systems.

20. Service Level Agreement (SLA) for Internal and External Information Technology Services

Information technology provisioning must maintain clear agreements between service users and service providers, both externally and internally, to establish standards, build mutual understanding, and enhance operational efficiency in alignment with strategic goals, categorized into 2 main groups as follows:

20.1 Qualifications of External IT Service Providers:

20.1.1 Service providers must establish and comply with a clear SLA, specifying scopes, durations, and system availability levels, alongside demonstrating expertise in relevant technologies.

20.1.2 Maintain comprehensive data security management systems that align with legal requirements and comply with the Personal Data Protection Act (PDPA).

20.1.3 Be capable of evaluating and reporting service performance based on Key Performance Indicators (KPIs) agreed upon with the organization.

20.1.4 Adapt and respond appropriately to the organization's requirements.

20.1.5 Maintain credibility, transparency, and possess agreements regarding data confidentiality (Confidentiality Agreement) and data ownership rights (Data Ownership).

20.2 Qualifications of Internal IT Service Providers:

20.2.1 Maintain personnel with knowledge, capabilities, and experience appropriate for assignments.

20.2.2 Establish and comply with clear internal SLAs between the service-providing unit and service-using units.

20.2.3 Maintain data security management systems, covering access, storage, backup, and cyber threat protection.

20.2.4 Support and respond efficiently to the requirements of internal departments.

20.2.5 Promote innovation and the adoption of modern technology to enhance organizational efficiency.

20.2.6 Maintain transparency, accountability, and manage risks appropriately.

21. Policy Review

The Information Systems and Data Communication Network Usage Policy shall be reviewed and presented to the Board of Directors for approval at least once a year.

It is hereby announced for general acknowledgment and strict compliance from the date of signing at the end of this announcement. This Information Systems and Data Communication Network Usage Policy was approved by the Board of Directors in Meeting No. 8/2025 on November 11, 2025.

Announced on November 25, 2025.
(Mr. Siwaphong Boonsalee)
Managing Director