Information Security Policy and Guidelines

Thai Rubber Latex Group Public Company Limited and Subsidiaries

1. Purpose and Scope

Thai Rubber Latex Group Public Company Limited and its subsidiaries have established an Information Security Policy and Guidelines to ensure that electronic operations with various departments are secure and reliable. The company's policy requires departments to establish written systems and procedures for information security to ensure that the IT systems of the Company (Thai Rubber Latex Group Public Company Limited and subsidiaries) operate correctly, appropriately, efficiently, and securely with continuity. This also prevents issues arising from incorrect IT usage and threats. The objectives are as follows:

1.1 To establish a policy for IT and communication security to ensure confidence and safety in using the company's IT systems or computer networks, leading to efficient and effective operations.
1.2 To define the scope of IT and communication security management based on ISO/IEC 27001 standards with continuous improvement.
1.3 To disseminate this policy to all levels of personnel, who must strictly comply.
1.4 To set standards, guidelines, and procedures for executives, system administrators, and external parties to recognize the importance of information security and strictly adhere to it.
1.5 To ensure systems and procedures are audited, reviewed, and evaluated at least once a year.

2. Policy Framework

2.1 **Access and User Rights Control**
- Section 1: Server Room Access Control
- Section 2: IT and Communication System Access Control
- Section 3: User Data Access Management
- Section 4: User Roles and Responsibilities
- Section 5: Network Service Access Control
- Section 6: Operating System Access Control
- Section 7: Application and Information Access Control
- Section 8: External Party Access Control

2.2 **System and Data Management**
- Section 9: System Acquisition, Development, and Maintenance Policy
- Section 10: Data Backup Procedures
- Section 11: System Installation and Configuration Guidelines

2.3 **Risk Management and Security Awareness**
- Section 12: Risk Assessment and Audit
- Section 13: IT Security Awareness Building

2.4 **Internet and E-mail Usage Policy**
- Section 14: Internet Usage Security Policy
- Section 15: E-mail Usage Guidelines
- Section 16: E-mail Service Agreement

2.5 **Physical and Environmental Security**
- Section 17: Physical and Environmental Security

2.6 **Emerging Technology Governance**
- Section 18: Cloud System Usage Control
- Section 19: Artificial Intelligence (AI) Usage Control

The Company's Information Technology and Communication Security Policy encompass objectives, standards, guidelines, and procedures designed to systematically maintain the security of its IT and communication systems.

This policy enables the Company to implement appropriate security measures, thereby mitigating risks and preventing potential damage to operations, assets, and personnel. Its primary goal is to ensure the overall security and continuity of the Company's business operations.

This Information Technology and Communication Access Policy constitute a mandatory Security Standard. All Company personnel and external parties are strictly required to comply with the provisions set forth herein.

Definitions

1. **Company:** Thai Rubber Latex Group Public Company Limited and Subsidiaries
2. **Subsidiaries:** Thai Rubber HPNR Co., Ltd., Thai Rubber Land and Plantation Co., Ltd., Latex Systems Public Company Limited, Thai Tex CBD Smart Farm Co., Ltd., and Wang Somboon Rubber Plantation Co., Ltd., which utilize the same network system as Thai Rubber Latex Group Public Company Limited.
3. **Information Security:** The maintenance of security for the information technology and communication systems of Thai Rubber Latex Group Public Company Limited and its subsidiaries.
4. **User:** Any individual granted rights or permission to access the organization's information systems, data, resources, or services, including employees, executives, customers, partners, or external parties. Usage must comply with the rights, duties, and policies defined by the organization.
5. **User Rights:** The scope or privileges granted to users of information systems or IT services, such as data access, program or system resource usage, data modification or recording, including rights to personal data protection and privacy. Such rights are determined based on security policies and organizational roles.
6. **Assets:** Data, Systems, IT and Communication Technology, and any resources of value or importance to organizational operations, both tangible (e.g., computers, peripherals, network systems, licensed software) and intangible (e.g., information, system licenses, technical knowledge). Assets must be maintained and protected to support business continuity and security.
7. **Access or Information Usage Control:** The definition of rights, duties, and methods by which users can access, use, modify, or manage information and systems under organizational security policies to prevent unauthorized access and mitigate data breach risks.
8. **Information Security:** The management, protection, and control of organizational data or information to prevent unauthorized access, use, disclosure, modification, or destruction, thereby maintaining Confidentiality, Integrity, and Availability (CIA) of data and information systems, including Privacy.
9. **Security Event:** Any occurrence or action involving information systems, data, or technology infrastructure that may affect Confidentiality, Integrity, or Availability of information, such as unauthorized access, data leaks, cyberattacks, or system failures impacting organizational operations.
10. **Unfavorable or unforeseen information security situations:** incidents or conditions that occur unintentionally and unexpectedly, resulting in a negative impact on the organization's information security. These include complex cyberattacks, emerging threats, unexpected system failures, natural disasters, or any event that causes damage to data, systems, or the organization's normal operations.

11. **External Party:** Organizations, Individuals, or entities outside the direct supervision of the main organization but involved in or having a collaborative operational relationship, such as partners, service providers, contractors, consultants, or relevant government agencies
12. **Password:** A string of characters, numbers, or symbols created by a user to verify their identity for accessing organizational systems, data, or services. Passwords should be stored securely, possess sufficient length and complexity, and be changed according to organizational policy.
13. **Computer Data:** Data or Information in digital form that is created, stored, processed, or managed by a computer system. This may include files, databases, programs, or data transmitted over a network, intended to support organizational operations and decision-making.
14. **Electronic Data**: Data, Information, or any documents created, stored, sent, or processed in an electronic format using computer systems, digital devices, or electronic communication networks. This encompasses files, text, images, audio, or video in digital form.
15. **Network System:** A group of interconnected computer devices, servers, communication equipment, and software designed to exchange data and resources within an organization or between the organization and external parties. Network systems facilitate efficient communication, data access, and collaboration.
16. **Information Technology (IT) System:** An integrated set of computer hardware, software, network systems, and personnel working together to collect, process, store, and distribute information to support the operations, decision-making, and management of the organization.
17. **Information System Workspace:** The areas or locations designated for the installation, operation, or access of information and communication technology systems. This includes computer equipment, servers, network devices, and various information resources, governed by control measures to ensure the security of data and systems.
18. **Data Owner**: An individual, department, or internal unit responsible for the management, oversight, and decision-making regarding specific data. This includes its creation, storage, access, usage, and protection to ensure that data is handled accurately, securely, and in compliance with organizational policies.
19. **Electronic Mail (E-mail):** Messages or information sent and received through electronic systems, such as the internet or computer networks, whether internally or externally. It is used for communication and information exchange between users.
20. **Malicious Code:** Programs or Software designed to damage, disrupt, gain unauthorized access, or otherwise adversely affect computer systems, data, or networks. Examples include viruses, Trojans, worms, or malicious scripts.
21. **Cloud System:** The use of information technology resources-such as data storage, processing power, or online systems-provided via the internet by external service providers. This replaces the need for self-managed hardware and software, reducing costs and management complexity while increasing flexibility for anytime, anywhere access.
22. **AI System:** Artificial Intelligence systems; technology that enables computers and machines to simulate human capabilities in thinking, learning, problem-solving, decision-making, and creativity. By processing vast amounts of data through methods such as Machine Learning and Deep Learning, AI creates models capable of intelligent analysis, prediction, and response.

Section 1: Server Room Access Control

1. Objective

To establish control and preventive measures for maintaining security regarding the use of or access to computer control rooms, network equipment, and information technology systems. These measures are determined based on the criticality of the equipment, IT systems, and data, which are considered valuable assets and may require confidentiality. This policy applies to all users involved in the operation of the Company's information and communication technology systems.

2. Access Control

2.1 The Company shall appropriately categorize and designate areas for servers, network equipment, and various information technology systems. These designations are documented in the "Information System Security Zone Classification," intended for surveillance and security control against unauthorized access and the prevention of potential damage.

2.2 The information technology and communication workspace must be clearly defined and partitioned. A layout plan indicating the location of these workspaces shall be established and communicated company widely. These areas are categorized into types such as General Workspaces, IT Equipment Installation Areas, and Data Storage Areas.

2.3 Access rights must be granted to personnel to allow them to enter designated areas to perform assigned duties, comprising the following:

- Maintain a "Register of Authorized Personnel" to ensure individuals access areas according to their assigned rights and responsibilities.
- Designate personnel responsible for recording such entries and exits via the "Area Access Log" (Fingerprint Scan).
- Assign responsible officers to regularly audit the access logs of the IT system workspaces. The list of authorized personnel for these workspaces must be reviewed and updated at least once a year.

2.4 External parties or visitors must register their entry and exit the authorized Access. Form and must be always accompanied by the contact person during their stay.

2.5 For any other personnel without direct responsibilities who request access to a restricted area, the department in charge of that area must verify the reason and necessity before granting permission.

Section 2: Information Technology and Communication Access Control

1. Objective

To establish control measures that prevent unauthorized access to the Company's IT and communication systems. This policy aims to protect against network intrusions and malicious software (malware) that may cause data damage or system disruptions, while ensuring accurate identification, authentication, and auditability of all system users.

2. Data Classification and Confidentiality Levels

2.1 Data Categories and Electronic Document Formats:

2.1.1 Text Formats: Files containing readable text generated by general software, including:

- TEXT Format: Plain text files without formatting (e.g., color, bold, or font styles).
- Document Format: Files created by word processors (e.g., Microsoft Word) that preserve both text and formatting. Compatibility may vary across software versions.

- PDF Format (Portable Document Format): Designed for cross-platform compatibility (Windows, macOS, Linux) while preserving original formatting. Requires specific software like Adobe Acrobat for viewing and creation.
- XML (Extensible Markup Language): A language used to structure documents via Metadata (Tags) to define data types and structures, facilitating seamless data exchange between systems.

2.1.2 Image Formats: Files generated by image-processing software, including:

- JPEG Format: Designed for multi-colored images using Lossy Compression to reduce file size; ideal for photographs.
- PNG / GIF Formats: Uses Lossless Compression; ideal for graphics, logos, or icons requiring high clarity and transparency support.
- Bitmap Format (BMP): Stores data as individual pixels; suitable for high-resolution images but results in large file sizes.

2.2 Data Confidentiality and Priority:

The Company applies appropriate management and security frameworks for electronic documents based on their importance:

- Confidentiality Levels: Classified into 3 levels: Confidential, Secret, and Top Secret. Authorized personnel are responsible for assigning, declassifying, or adjusting these levels as necessary.
- Document Control: Measures include registration, auditing, documentation, copying, translation, transmission/receipt, storage, borrowing, destruction, emergency protocols, and information disclosure.

3. Core Access Control Processes

3.1 Critical IT infrastructure locations must have stringent physical access controls, limited only to authorized personnel.

3.2 Administrators must assign access rights based on the "Principle of Least Privilege" and job responsibilities. Access rights must be reviewed regularly.

3.3 Only administrators or designated personnel are authorized to modify access rights.

3.4 Administrators must implement logging and monitoring systems to track IT usage and detect security breaches.

3.5 Records of system access, modifications, and physical entry/exit (both authorized and unauthorized) must be maintained for audit purposes.

4. IT System Access Control

4.1 Administrators are responsible for verifying approvals and granting access. Requests for system access must be documented, signed by authorized supervisors, and archived as evidence.

4.2 Data/System Owners shall grant access based on a "Need-to-Know" basis. Excessive privileges are prohibited to mitigate the risk of unauthorized actions.

4.3 Users must obtain official permission from relevant data and system authorities before accessing IT resources.

5. User Access Management

5.1 Registration: A formal process is required for new staff. Users request access, supervisors approve, and administrators manage the account.

5.2 Termination: Access rights must be revoked within 24 hours of resignation or within 7 days of internal job rotation.

5.3 Privileged Systems: Access to critical systems (e.g., Applications, E-mail, Wireless LAN, Internet) require written approval from the administrator and periodic reviews.

5.4 Accountability: Users must sign a formal acknowledgment of their rights and duties, strictly adhere to the policy, and keep passwords confidential.

5.5 Password Security Standards:

5.5.1 Minimum length of 8 characters, including a mix of uppercase, lowercase, numbers, and symbols.

5.5.2 Avoid personal information (names, family, birthdays) or dictionary words.

5.5.3 Does not use personal passwords for shared network folders.

5.5.4 Does not use "Auto-save Password" features on workstations.

5.5.5 Does not record passwords in visible or easily accessible locations.

5.5.6 Initial passwords must be complex and delivered securely.

5.6 User Account & Credential Management:

5.6.1 Administrators must define rights per functional roles as specified in "Section 3: User Access Management."

5.6.2 Modifications and revocations must follow the established Section 3 procedures.

5.6.3 Privileged Accounts (Super Users): Must be strictly controlled:

- Requires supervisor approval and administrator consent.
- Used only when necessary.
- Access is time-bound and must be suspended immediately after the task.
- Passwords must be changed immediately after use or every 6 months for long-term tasks.

5.7 Classification-Based Access Management:

5.7.1 Administrators define storage and destruction methods per confidentiality level.

5.7.2 Data owners must review user access rights at least once a year.

5.7.3 Identity verification (Username/Password) is mandatory for accessing classified data.

5.7.4 Transmission of sensitive data over public networks must use international standard Encryption.

5.7.5 Passwords must be changed according to the intervals defined in Section 3

5.7.6 Off-site equipment security: Before sending computers for external repair, data must be backed up, and storage media must be wiped.

6. Network Access Management

6.1 Network architecture must be segmented (e.g., Internal Zone, External Zone) to systematically control and prevent intrusion.

6.2 Administrators must implement restrictions ensuring users access only authorized network segments.

6.3 Access paths to shared networks should be limited.

6.4 Enforced paths from clients to servers must be established to prevent the use of unauthorized routes.

6.5 Configuration parameters for network devices must be reviewed at least once a year. Any changes must be communicated to stakeholders.

6.6 External connections must pass through intrusion prevention devices (Firewalls) with packet filtering and Malware detection capabilities.

6.7 IPS/IDS (Intrusion Prevention/Detection Systems) must be installed to monitor and alert on abnormal network activities or unauthorized modifications.

6.8 Remote access to the internal network via the Internet requires secure login and multi-factor authentication.

6.9 Internal IP addresses must be masked from external parties to prevent network mapping.

6.10 Maintain and update a Network Diagram detailing internal and external boundaries.

6.11 Network monitoring tools must be approved by administrators and used only as necessary.

6.12 Installation and connection of network devices must be performed exclusively by the AI/IT department.

7. Server Management

7.1 Designated personnel must be clearly assigned to manage server and system software configurations.

7.2 Standard procedures for monitoring server health and detecting unauthorized changes must be implemented, with immediate reporting protocols.

7.3 Only essential services (e.g., Telnet, FTP, Ping) should be enabled. Risk-prone services require additional security measures.

7.4 System software (e.g., Web Servers) must be regularly updated with the latest security patches.

7.5 Security and performance testing must be conducted before and after server maintenance or installation.

7.6 Server installation and connectivity must be handled by the AI/IT department only.

8. Logging and Auditing Management

8.1 Administrators must maintain logs for servers, networks, applications, and security systems (e.g., Command Line, Firewall logs). Logs must be retained for at least 3 months.

8.2 User activity logs must be reviewed regularly.

8.3 Logs must be protected against unauthorized modification, with access restricted to relevant personnel only.

9. Remote Access Control

9.1 Security controls must be implemented for external access to internal systems.

9.2 Remote Access requires enhanced security measures beyond standard internal login protocols.

9.3 Remote access methods must be approved by the AI/IT department and strictly monitored.

9.4 Users requesting remote access must provide sufficient business justification and obtain formal authorization.

9.5 Ports used for remote access must be strictly controlled and secured.

9.6 Remote access is granted on a necessity basis; ports should be closed when not in use and opened only upon authorized request.

10. Authentication for External Users

All users accessing the system from external locations must undergo organizational authentication:

10.1 Provide a Username.

10.2 Provide a Password.

Section 3: User Access Data Management

1. Objective

To establish control measures for accessing IT systems, ensuring that unauthorized individuals are prevented from accessing internal networks and IT resources. This policy also aims to restrict usage rights to a necessary level and ensure the ability to track, monitor, and authenticate individuals accessing the Company's IT and communication systems.

2. User Registration

2.1 Standardized user registration forms must be developed for all Company IT systems.

2.2 Administrators must verify user accounts to ensure no prior duplicate registration exists.

2.3 Administrators must review and grant access rights that are appropriate to the user's specific roles and responsibilities.
2.4 Administrators must provide written documentation to users outlining their access rights, duties, and responsibilities. Users are required to sign this document after acknowledging the terms.
2.5 Access rights must be revoked immediately upon a user's resignation or change in job position.
2.6 Administrators must periodically audit all user accounts to prevent unauthorized access to IT systems.

3. User Management

3.1 Administrators should define IT system access rights based strictly on functional necessity and conduct regular reviews of these rights.
3.2 Appropriate access privilege levels must be established for each IT system.
3.3 The assignment of privileges must be consistent with the Company's User Access Control Policy.
3.4 Records of all privilege assignments must be maintained.
3.5 Privileged Access (Super Users): Special access for high-level users must be time bound. Access must be suspended immediately upon the expiration of the designated period or when the user leaves the position. Specific levels of access must be clearly defined, and privileged account credentials must be distinct from regular user credentials.

4. Password Management System

4.1 The password management system must require unique individual accounts and passwords to ensure accountability and traceability for each user.
4.2 The system must allow users to select or change their own passwords and include a verification step for new password settings.
4.3 The system must enforce the use of complex passwords that are difficult to guess (e.g., avoiding names of parents, relatives, or common dictionary words).
4.4 The system must mandate periodic password changes, such as every 6 months.
4.5 Users must be required to change their password immediately upon their first login with a new account.
4.6 The system must mask password characters on the screen during the login process (e.g., using dots or asterisks).
4.7 Passwords stored within the system or transmitted over the network must be protected using international security standards, such as Hashing, to prevent unauthorized access.

5. User Password Management

5.1 Administrators must require users to sign a non-disclosure agreement regarding their passwords (e.g., signing a duty and responsibility acknowledgment form).
5.2 Formal procedures for setting or changing passwords must be established.
5.3 Users must change their password immediately after receiving a temporary password, choosing a new password that is difficult to guess.
5.4 Temporary passwords generated by administrators must be complex and unique for each instance.
5.5 Temporary passwords should be delivered through secure channels, avoiding plain-text email where possible, and users must confirm receipt.

6. Review of User Access Rights

6.1 Administrators must conduct a formal review of user access rights at least once a year.

6.2 High-level privileges, such as Administrator rights, must be reviewed more frequently than standard user accounts.

6.3 Access rights must be reviewed at scheduled intervals or whenever significant changes occur, such as promotions, demotions, departmental transfers, or termination of employment.

6.4 All changes to high-level privileged accounts must be logged and recorded for future audit and review purposes.

Section 4: User Responsibilities

1. Objective

To establish and enforce operational measures governing user activities related to information assets. This policy applies to all individuals utilizing the Company's IT systems to prevent unauthorized access and protect against the non-consensual disclosure of information.

2. Password Usage

2.1 All IT system users must adhere to the following password security requirements:

2.2 Users must create passwords that are difficult for others to guess.

2.3 Users must never disclose their passwords to anyone.

2.4 Users must store password-related information in a secure location.

2.5 Users must change their password immediately if they suspect it has been compromised or disclosed to others.

2.6 Users are encouraged to create passwords that exceed the minimum required length.

2.7 Users should utilize mnemonic techniques to ensure their passwords are easy to remember without being easy to guess.

2.8 Users must not use common dictionary words as passwords.

2.9 Users must avoid sequential characters (e.g., 123, abcd) or repetitive character strings (e.g., 111, aaa).

2.10 Passwords must be changed according to the scheduled rotation cycles.

2.11 When changing a password, users must not reuse previously used passwords.

2.12 Administrators must change their passwords more frequently than standard users (e.g., every 3 months for Administrators and every 6 months for general users).

2.13 Temporary passwords must be changed immediately upon the first login to the system.

2.14 Users must not enable "Remember Password" or "Autofill" features for login convenience.

2.15 Users are strictly prohibited from sharing their personal passwords with others.

2.16 Users should avoid using the same password across multiple different systems or applications.

3. Unattended Equipment Protection

3.1 Users must log out or terminate their sessions immediately upon completion of their tasks, including applications, workstations, and laptops.

3.2 Users must lock their devices (Screen Lock) whenever they are away from their desk or leaving the equipment unattended temporarily.

3.3 Administrators must enforce security configurations that require a password or secure authentication to unlock a computer or re-access IT systems after a period of inactivity.

Section 5: Network Access Control

1. Objective

To establish control measures that prevent unauthorized personnel from accessing, perceiving, modifying, or tampering with critical network and communication systems, which could result in damage to the Company's data and information systems. Access control is managed through network segmentation, such as Virtual Local Area Networks (VLANs), tailored to specific network groups.

2. Network Access and Service Control Process

2.1 Utilization of Network Services:

2.1.1 Legal and Ethical Compliance: Users are strictly prohibited from performing any actions involving data that are illegal or contrary to public morality. The user acknowledges that any such actions are outside the scope of the Company's responsibility.

2.1.2 Prohibition of Commercial Use: The Company prohibits the use of its computers and networks for commercial gain or profit-seeking activities. This includes, but is not limited to, advertising, buying/selling goods, trading data, providing fee-based information searches, or offering internet services to the public for profit.

2.1.3 Non-Violation of Others' Rights: Users must not read, write, delete, or modify any data that does not belong to them without authorization. Hacking into another person's User Account, disseminating defamatory content, or using offensive language is strictly prohibited. The user shall be solely liable for any damage resulting from such violations.

2.1.4 Unauthorized Access: Unauthorized access or attempted intrusion (hacking) into the system is considered a violation of the Company's restricted areas.

2.1.5 Individual Accountability: User Accounts are provided exclusively for individual use. Users must not transfer or distribute their access rights to others.

2.1.6 Responsibility for Account Activity: Users are responsible for all activities and potential damages originating from their User Account, unless it can be proven that the damage was caused by another party.

2.1.7 Prohibited Software: Use of Peer-to-Peer (P2P) file-sharing or high-risk software is prohibited unless authorized by a supervisor.

2.1.8 Entertainment Policy: Use of any online programs for entertainment purposes during working hours is strictly prohibited.

2.2 Guidelines for Network Administrators and Staff:

2.2.1 Access Authorization: The Network Room Administrator must define access rights for authorized personnel (e.g., Computer Operators, System Administrators) and maintain a "Restricted Area Access Registry."

2.2.2 Formal Approval: Entry into specific zones within the network control room requires written approval from the AI/IT Department, based on the individual's job functions.

2.2.3 Entry/Exit Logging: All entries and exits must be recorded according to the "Area Entry-Exit Form" process.

2.2.4 Control of Non-Regular Personnel: Stringent controls must be applied when non-regular personnel require access to the network control room for specific tasks.

2.2.5 Record Keeping: Every instance of access to the network control room must be documented in the "Area Entry-Exit Form."

2.3 Guidelines for External Visitors/Contractors:

2.3.1 Mandatory Logging: All external visitors must record their information in the "Area Entry-Exit Form" logbook.

2.3.2 Equipment Registration: Visitors bringing computers or technical tools into the network control room must clearly list all items in the authorized entry-exit form.
2.3.3 Periodic Audits: Staff should verify the accuracy of the logbook entries monthly.

2.4 Network Device Identification:
2.4.1 Connection Registry: Administrators must maintain a registry of network connection requests, including usernames, computer specifications, IP addresses, and installation locations.
2.4.2 External Device Identification: Devices connected from external networks must be identified to determine whether they are authorized to access the internal network.
2.4.3 IP Traceability: Network devices must be capable of identifying and auditing both source and destination IP addresses.
2.4.4 Request Form: All users must complete a "Network Connection Request Form" before being granted access.

2.5 Protection of Diagnostic and Configuration Ports:
2.5.1 Port Management: Administrators must manage the opening and closing of network device ports. High-risk ports that could compromise network security must remain closed.
2.5.2 External Supervision: Third parties entering the computer control room must be authorized by the AI/IT Head and must be always accompanied by Company staff.
2.5.3 Port Maintenance Approval: Any third-party maintenance or remote management of network device ports requires hierarchical approval from management.
2.5.4 Service Deactivation: Unnecessary ports and services on network devices must be disabled or deactivated.

2.6 Network Segmentation:
2.6.1 Physical and Logical Segregation: The network is segmented by buildings/units to control unauthorized access effectively.
2.6.2 Internal and External Zone Separation: To ensure database security, internal systems are accessible only via the internal network. External access to these core systems is restricted.
2.6.3 Firewall Implementation: Firewalls are installed at all network entry points to protect the Company's infrastructure from malicious actors.

Section 6: Operating System Access Control

1. Objective

To ensure that all users acknowledge their roles and responsibilities regarding the use of operating systems. This policy requires users to understand and strictly adhere to established protocols to safeguard organizational resources and data, maintaining Confidentiality, Integrity, and Availability (CIA) always.

2. Secure Operating Procedures for Access

2.1 Personal Password Requirement: Users must set a secure password for accessing the computer systems under their responsibility.
2.2 Screen Lock Policy: Users must configure a screen saver with a password lock that activates during periods of inactivity. Re-entry of the password is required to resume sessions.
2.3 Mandatory Identification: Users must provide a unique Username and Password every time before accessing the operating system.
2.4 Prohibition of Credential Sharing: Users are strictly prohibited from sharing their Username and Password with others to access organizational computer systems.
2.5 Mandatory Logout: Users must logout immediately upon finishing their tasks or when leaving their workstation for an extended period.

2.6 High-Risk Software Restriction: The use of Peer-to-Peer (P_2P) file-sharing or high-risk software is prohibited unless specifically authorized by a supervisor.
2.7 Software License Compliance: The Company utilizes licensed software based on functional necessity. Installation or use of unlicensed software is strictly prohibited. Any violation is considered a personal liability of the user.
2.8 Software Integrity: Users must not install, uninstall, alter, modify, or duplicate any software provided by the Company for use elsewhere.
2.9 Commercial Use Prohibition: Company resources of all types must not be used for commercial or personal profit-seeking activities.
2.10 Content Standards: When creating web content on the corporate network, users are prohibited from presenting illegal, copyrighted, inappropriate, or immoral information and images.
2.11 Unauthorized Remote Control: Using the Company's IT systems to control external computers or information systems without official authorization is prohibited.

3. User Identification and Authentication

3.1 Mandatory Authentication: Users must authenticate their identity every time they access IT systems to prevent unauthorized access. Any errors or issues during the identification process must be reported to the system administrator immediately for resolution.
3.2 Accountability: The account owner is solely responsible for all actions and consequences arising from the use of their account within the computer and network systems, unless it can be proven that the damage was caused by a third party.
3.3 Credential Confidentiality: Users must keep their account credentials confidential and are prohibited from transferring, selling, or distributing them to others without supervisory approval.
3.4 Session Management: Users must log in using their own credentials and log out every time they finish their work or pause their activities.

4. Use of System Utilities

4.1 Utility Access Control: Procedures must be established for requesting approval to use system utilities. This includes defining approval levels and requiring authentication to limit and control the use of these tools.
4.2 Separation of Environments: System utility programs must be stored separately from application software.
4.3 Restricted Access: Access to system utilities is restricted only to specifically authorized personnel.
4.4 Software Minimization: Unnecessary utility programs and software related to application systems must be removed or deleted. Measures must be implemented to prevent unauthorized users from accessing or executing system utilities.

Section 7: Application and Information Access Control

1. Objective

To establish control measures that prevent unauthorized access to the Company's information systems and protect against network intrusions or malicious scripts. This policy aims to safeguard data integrity, prevent system disruptions, and ensure accurate tracking and authentication of all users accessing the Company's IT and communication infrastructure.

2. Information Access Control

2.1 User Lifecycle Management: Administrators must implement formal procedures for the registration of new personnel, granting only necessary access rights. Formal protocols must also be established for the timely revocation of rights due to resignation or internal job rotation.

2.2 Privileged System Access: Access to critical resources (e.g., core Applications, E-mail, Wireless LAN, and Internet) is restricted to functional requirements and requires written approval from a direct supervisor. Access rights must be reviewed regularly.

2.3 Session Timeout: A "Limitation of Connection Time" must be implemented. If the system remains idle for more than 10 minutes, the session will automatically terminate, and the user must log in again.

2.4 Credential Management: Administrators are responsible for the following:

- 2.4.1 Revoking passwords immediately upon a user's resignation or termination of duties.
- 2.4.2 Securely delivering temporary passwords; avoiding plain-text emails or delivery via third parties.
- 2.4.3 Requiring users to confirm receipt of new passwords.
- 2.4.4 Prohibiting users from storing passwords in an unprotected format on any computer system.
- 2.4.5 Ensuring every User ID or Username is unique.
- 2.4.6 Privileged Users (Super Users): High-level access requires supervisor approval, is strictly time-bound, and must use credentials distinct from standard accounts. Access must be suspended immediately upon completion of the task or change in role.

2.5 Internal Web-Base Application Security: Critical web-based applications are restricted to the Company's internal network and accessible only from authorized office locations.

2.6 Classification-Based Access: Administrators must manage access based on data confidentiality levels, covering direct access, application-level access, and data destruction methods:

- 2.6.1 Control access according to the assigned confidentiality level of the data.
- 2.6.2 Enforce Username and Password verification for all classified data access.
- 2.6.3 Terminate access immediately upon expiration of the authorized period. Transmission of sensitive data over public networks must use international encryption standards (e.g., SSL VPN, XML Encryption).
- 2.6.4 Rotate passwords based on the sensitivity and classification level of the information.
- 2.6.5 Secure off-site equipment: Before sending devices for external repair, sensitive data must be backed up and securely wiped from the storage media.

3. Limitation of Connection Time

3.1 IT systems must enforce a maximum connection duration. Standard sessions are limited to 1 hour per connection and are restricted to normal office operating hours.

3.2 High-priority systems or systems accessed from high-risk locations (public areas or off-site) must have strictly defined connection windows.

3.3 Systems requiring time-limited access must prompt re-authentication every 1 hour.

4. Teleworking (Working from Outside the Office)

4.1 Before authorizing remote work, necessary security measures and physical environment assessments must be completed for the remote site.

4.2 Secure communication channels between the remote site and the internal corporate systems must be established before teleworking commences.

4.3 Physical security measures at the remote location (including the building and environment) must be verified to prevent equipment theft, unauthorized data access, or malicious remote intrusions.

4.4 Control must be established for home network usage, including security standards for personal wireless routers.
4.5 Personal devices used for remote access must meet the Company's requirements for antivirus protection and firewall configurations.
4.6 Remote workers must be provided with necessary equipment, secure data storage, and communication tools by the Company.
4.7 Remote access via personal devices is strictly prohibited unless the device is under Company-authorized management and supervision.
4.8 The Company shall define the types of work permitted for teleworking, authorized working hours, data confidentiality levels allowed, and the specific applications or services accessible remotely.
4.9 Procedures must be established for the application and termination of teleworking status, modification of access rights, and the return of Company equipment upon cessation of remote work.

Section 8: Third-Party Access Control

1. Objective

Engaging with third-party service providers may introduce significant risks, such as unauthorized data access, improper data modification, or unauthorized system processing. This policy aims to ensure that third-party access to the Company's IT and communication systems is managed securely. It establishes guidelines for selecting and supervising external entities, including software developers, consultants, and IT service providers.

2. Operating Guidelines

2.1 Risk Assessment: The Head of the AI/IT Department must ensure that a comprehensive risk assessment is conducted regarding third-party access to IT systems or processing equipment. Appropriate mitigation measures must be implemented before any external access is granted.
2.2 Third-Party Access Control Protocols:
2.2.1 Formal Authorization: Any external party requiring access to the Company's IT and communication systems must submit a formal written request for approval to the Head of the AI/IT Department.
2.2.2 Documentation Requirements: A standardized request form must be utilized by third parties to justify the necessity of access. The form must include, at a minimum, the following details:
- Purpose of access.
- Authorized duration of access.
- Security verification of connected equipment.
- MAC Address verification of connecting computers.
- Non-disclosure and data protection protocols.

2.2.3 Non-Disclosure Agreement (NDA): Every third-party entity working for the Company, whether on-site or off-site, must sign a Non-Disclosure Agreement. This agreement must be finalized and executed before any system of access rights are granted.
2.2.4 External Risk Audits: Depending on the criticality of the systems involved, the Company may conduct risk assessments or audit the internal controls of the third-party provider.
2.2.5 Principle of Least Privilege: Project owners responsible for external collaborations must restrict access to authorized personnel only and ensure all participating external staff have signed NDAs.

2.2.6 Security Framework for Major Projects: For large-scale projects involving access to critical data, Administrators must ensure that third-party operations adhere to the five pillars of information security:
- Confidentiality: Protection against unauthorized disclosure.
- Integrity: Safeguarding against unauthorized modification.
- Availability: Ensuring systems are accessible when needed.
- Non-repudiation: Ensuring actions cannot be denied later.
- Compliance: Adherence to relevant regulations and laws.

2.2.7 Right to Audit: The Company reserves the right to audit third-party activities as stipulated in the service agreement to ensure comprehensive oversight and compliance with security standards.

2.2.8 Operational Documentation: Third-party providers should be required to provide project plans, operating manuals, and related documentation. These materials must be kept up-to-date to facilitate strict monitoring and ensure service delivery remains within the defined scope.

Section 9: System Procurement, Development, and Maintenance Policy

1. Objective

To establish policies and operating procedures for the procurement, development, and modification of information systems, ensuring all activities are correctly governed and supervised by System Administrators.

2. Guidelines for Software Procurement and Development

2.1 Technical Involvement and Analysis: System Administrators must be involved in the procurement process for all software. A comprehensive analysis must be conducted to justify the selection, ensuring that the chosen solution can support the organization's future operational requirements and scalability.

2.2 Selection Methodology: The selection of software must receive formal approval from System Administrators. Procurement methods may include:
a. Off-the-shelf (Packaged) Software: Ready-made solutions.
b. Customized Software: Tailored solutions developed by external vendors.
c. In-house Development: Systems developed internally by the Company.

2.3 User Acceptance Testing (UAT): All procured or developed software must undergo rigorous testing by both end-users and System Administrators. This process aims to identify errors and assess practical suitability based on predefined evaluation criteria.

2.4 Impact Assessment: Before final approval for procurement or development, an impact assessment must be conducted to evaluate potential effects on hardware, existing software, and end-user workflows.

2.5 Centralized Installation: Once approved, all software installations—including testing environments and version upgrades—must be performed exclusively by authorized System Administrators.

3. Guidelines for System or Report Maintenance and Modification

3.1 Formal Request Process: The Company has established formal procedures for requesting system modifications or new reports. All requests must be submitted using the designated request forms.

3.2 Responsibility and Verification: Specific personnel shall be assigned responsibility for installing system updates or modified reports. Updated reports must be verified and signed off by users before final implementation.

3.3 Data Backup: A full system and report back-up must be performed before any new updates or modifications are applied to the production environment.
3.4 System Integrity: Modifications to systems or reports must be executed carefully to ensure they do not adversely impact other existing systems, databases, or reporting structures.

Section 10: Data Backup and Recovery System

1. Objective

To establish standard protocols for data backup and system recovery, ensuring that System and Network Administrators can perform backups correctly and restore systems effectively when necessary.

2. Guidelines for Data and Computer System Backup

2.1 Regular Backups and Testing: Administrators must ensure that data backups and restoration tests are conducted regularly, strictly adhering to the Company's Backup Policy.
2.2 Operator Logs: Administrators must maintain detailed backup logs, including start and end times, the name of the individual performing the backup, and the type of data recorded.
2.3 Standard Procedures: Formal procedures for both software and information system backups must be established, with specific protocols tailored to each individual information system.
2.4 Fault Logging: Any errors occurring during the backup process must be logged, including the corrective actions taken to resolve the issue.
2.5 Delegation of Duties: Backup responsibilities must be delegated to alternative personnel to ensure continuity if the primary System or Network Administrator is unavailable.
2.6 Issue Reporting: If a backup cannot be completed successfully, the administrator must resolve the issue, summarize the outcome, and report to the Head of the AI/IT Department.
2.7 Backup Strategy: Administrators shall determine appropriate backup types, schedules, and storage media. The two primary backup methods used are Full Backup and Incremental Backup.
2.8 Encrypted Backup: Critical backup data must be encrypted using appropriate technology to prevent unauthorized disclosure of the archived information.
2.9 Policy Compliance: All administrators must strictly comply with the established Backup Policy and Backup Procedures.

3. Backup Operations

3.1 Backup Frequency: Administrators must perform backups according to the following schedule:
3.2 Verification: Administrators must personally verify the backup results to ensure that all data is complete and accurate according to the schedule.

4. System Recovery

4.1 Emergency Recovery: In the event of system or network damage requiring recovery, administrators must execute the recovery plan, log the details, and report the summary to the Head of AI/IT or a designated representative.
4.2 Data Integrity: Use the Latest Update of the backed-up data for restoration, or as deemed appropriate for the situation.
4.3 User Notification: If a system failure affects user services, administrators must notify users immediately and provide periodic progress updates until the recovery is complete.
4.4 Recovery Drills: System recovery simulations and drills must be conducted at least once a year.

5. IT Contingency Plan

To mitigate risks from uncertainties and disasters that may impact databases and information systems, designated personnel must perform the following:

5.1 Planning: Establish a formal disaster response planning process for high-priority systems.

5.2 Threat Identification: Identify the types of disasters (e.g., natural, technical, or human error) that could impact critical systems.

5.3 Risk Assessment: Evaluate the potential risks and impacts that could lead to system downtime or unavailability.

5.4 Plan Development: Formulate a comprehensive IT Disaster Recovery Plan (DRP) for all high-priority systems.

5.5 Maintenance: Test, evaluate, and update the disaster response plan at least once a year to ensure its effectiveness.

Section 11: System Installation and Configuration Guidelines

1. Operating System (OS) Updates and Installation

1.1 Audit servers and system hardware components.

1.2 Install the operating system in accordance with functional requirements.

1.3 Configure credentials for the System Administrator and standard users.

1.4 Configure the Computer Name and IP Address settings.

1.5 Update and configure OS security levels (apply Service Patches and Updates).

1.6 Install Antivirus software, update virus definitions, and configure system scanning and auto-update schedules.

2. User Account and Access Management

2.1 Define and secure System Administrator credentials.

2.2 Define unique Usernames and Passwords for all users.

2.3 Maintain a registry of all user accounts and their associated system access rights.

3. System Security and Antivirus Updates

3.1 Monitor and audit computer operations and system access through Log Files, Performance Monitors, and installed security systems.

3.2 Adjust and update security configurations in response to emerging threats or issues.

3.3 Update Antivirus software and definitions weekly and conduct regular full-system virus scans.

4. Database Management System (DBMS) Operations

4.1 Install the Database Management System based on departmental requirements and service support needs.

4.2 Configure the database system or software to integrate seamlessly and efficiently with the Operating System, following vendor specifications.

4.3 Create and define Database Administrator (DBA) accounts, user accounts, and respective access privileges.

4.4 Regularly update and optimize system configurations to prevent performance issues and security vulnerabilities.

5. Application and Database Deployment

5.1 Install service-related software or applications based on business needs or development plans.

5.2 Configure programs and services for optimal compatibility and performance with the Operating System.

5.3 Deploy databases, establish application connections, and conduct functional service testing.
5.4 Notify users or system owners of availability by providing credentials and access rights as defined by the system.
5.5 Establish criteria for Backup, Copying, and Restore Testing.
5.6 Document all configuration settings, installation parameters, and user account levels whenever a system is created or updated.

6. Database Backup and Restore Operations

6.1 Monitor the performance of service programs and applications utilizing the database.
6.2 Audit database system operations and storage capacity at scheduled intervals (Daily or Weekly).
6.3 Verify the health and capacity of storage devices to ensure continuous service availability.
6.4 Perform Database Backups to designated storage media.
6.5 Standardize backup file naming: [Database Name] + [Backup Date].
6.6 Duplicate backup files as required and transfer them to designated storage units.
6.7 Conduct scheduled Restore Tests from backup files.
6.8 Execute full database restoration from the latest backup in the event of data corruption or system failure.
6.9 Maintain a comprehensive log for every operation, including Backup Name, Restore Test results, Action Level, Date, Success/Failure status, Operator Name, and Destination Area.
6.10 Promptly notify supervisors, system owners, and database users regarding any damage, corrective actions, restoration status, and system availability.

7. Hardware Maintenance and Inspection

7.1 Inspect physical server components, including general system status, Hard Disks, System Fans, LEDs, Monitors, and peripherals.
7.2 Clean hardware and equipment periodically according to the maintenance schedule.
7.3 Verify the operational status of the Uninterruptible Power Supply (UPS) where applicable.
7.4 Monitor system performance using OS Device and Performance Monitors, specifically tracking CPU usage, Memory, and remaining Hard Drive capacity.
7.5 Report all inspection results and identify issues to the System Administrator.
7.6 Document every inspection, repair, and maintenance activity performed.

Section 12: Monitoring and Risk Assessment

1. Objective

To establish risk control measures and prevent incidents that may impact information security.

2. Risk Assessment Guidelines

2.1 Information and Database Risk Management Process:

The Company utilizes the PDCA (Plan-Do-Check-Act) cycle to manage information security risks as follows:

2.1.1 Establish the Information Security Management System (Plan):

- Define the scope of the management system based on the Company's operations, locations, assets, and technology.
- Formulate a security policy covering the defined scope.
- Establish formal risk management procedures for all information assets.
- Conduct risk assessments, select risk treatment options, and define risk reduction standards (leveraging ISO/IEC 27001 controls).

- Present an overview of the risk landscape and obtain formal approval for residual risks.
- Develop the Statement of Applicability (SoA).

2.1.2 Implement the Management System (Do):

- Develop and execute a Risk Treatment Plan.
- Define metrics to measure the effectiveness of the security management system.
- Implement training and awareness programs for all personnel within the scope to ensure high efficiency and security compliance.
- Manage operations and resource allocation in accordance with the security policy.
- Establish Security Incident Management Procedures and enforce compliance among relevant parties.

2.1.3 Monitor and Review of the Management System (Check):

- Execute monitoring procedures (as defined in the security policy) to detect processing errors, security breaches, or attempted intrusions.
- Conduct regular reviews of the management system, incorporating audit results, incident logs, performance metrics, and stakeholder feedback.
- Regularly evaluate the effectiveness of the system against established KPIs and targets.
- Review risk assessments periodically (every 3-6 months) to account for changes in technology, business objectives, emerging threats, legal regulations, or social shifts.
- Perform internal security audits according to the defined schedule.
- Maintain records of actions and meetings (e.g., Management Security Reviews) to ensure accountability and auditability.

2.1.4 Improve the Management System (Act):

- Update the management system based on monitoring and reviewing results. This includes implementing management meeting resolutions, updating policies, correcting non-conformities, and strengthening measures to prevent recurring incidents.
- Communicate all updates and improvements to relevant departments with appropriate detail and verify the effectiveness of the changes.

2.2 Risk Management Planning for Databases and Information Systems:

The Company must do the following:

2.2.1 Manage risks to prevent or minimize damage, including maintaining Backup & Recovery capabilities for system restoration.

2.2.2 Develop an IT Contingency Plan to address uncertainties and disasters.

2.2.3 Maintain robust security systems for databases, such as Anti-Virus and Uninterruptible Power Supplies (UPS).

2.2.4 Define and enforce Access Rights for users at all levels.

2.3 Annual Review: The risk management system for databases and information systems must be reviewed at least once a year.

2.4 Audit and Assessment Requirements: The Company is required to produce and maintain documentation for the following:

2.4.1 Evidence of security policy reviews.

2.4.2 Written Information Security Policies approved by the CIO or CEO.

2.4.3 Defined roles and responsibilities for information security personnel.

2.4.4 A comprehensive inventory of all information systems within the organization.

2.4.5 Details of security systems protecting databases and information.

2.4.6 A detailed IT Contingency Plan.

2.4.7 Evidence of activities performed in accordance with the IT Contingency Plan.
2.4.8 Accurate and up-to-date Access Rights records for at least one core system.

Section 13: Information Security Awareness

1. Objective

To disseminate security policies and practical guidelines to all personnel and relevant stakeholders. The goal is to ensure they possess the necessary knowledge and understanding, recognize the critical importance of information security, and can implement security measures correctly in their daily operations.

2. Information Security Awareness Guidelines

2.1 Integrated Training Programs: Regularly conduct training sessions on policy compliance by integrating security guidelines into various corporate training curricula as part of the departmental training plan.

2.2 Comprehensive Staff Training: To propagate information security policies and foster awareness, the Company provides training for both existing and new employees at least once a year. These sessions focus on IT-related security and may feature guest speakers with expertise in information security to share specialized knowledge and industry best practices.

2.3 Security Communication & Campaigns: Display public relations materials and educational content, such as "Security Tips" or "Precautions," in formats that are easy to understand and implement. These materials should be updated frequently to address evolving threats.

2.4 Engagement & Evaluation: Encourage active participation and practical application through consistent monitoring, performance evaluation, and user requirement surveys to ensure the awareness program remains effective and responsive to user needs.

Section 14: Internet Security Policy

1. Objective

To ensure that all users acknowledge the rules and guidelines for safe internet usage and to prevent violations of the computer-Related Crime Act. This includes prohibiting the transmission of data, messages, or commands that disturb the peaceful use of systems by others or cause the Company's computer systems to be suspended, delayed, obstructed, or disrupted from normal operation.

2. Internet Usage Guidelines

2.1 Secure Connectivity: Administrators shall designate specific network paths for internet access, which must pass through the Company's provided security systems (e.g., Proxy, Firewall, IPS/IDS). Users are strictly prohibited from connecting through unauthorized channels unless there is a business necessity and written permission has been obtained from the IT Department.

2.2 Device Compliance: All workstations and laptops must have antivirus software installed and the latest operating system and browser security patches applied before connecting to the internet via a web browser.

2.3 Patch Management: Users must regularly update patches and hotfixes. Critical updates should be downloaded from official sources, such as the Microsoft website, to remediate known system vulnerabilities.

2.4 Data Transmission Security: All data transmitted or received via the internet must undergo a virus scan using the Company's authorized antivirus software prior to every transaction.

2.5 Prohibited Content: Users must not utilize the Company's internet network for personal business gain or access inappropriate websites, including those that are immoral, socially harmful, or contain content against the Nation, Religion, or Monarchy.

2.6 Access Control: User access to internet resources is granted based on job responsibilities to ensure network efficiency and the security of corporate data.

2.7 Ethical Use: Users must not disseminate information for personal benefit, content that is immoral, or data that violates the rights of others or could cause reputational damage to the Company.

2.8 Confidentiality: Users are strictly prohibited from disclosing sensitive or confidential corporate information that has not been officially announced via the internet.

2.9 Image Integrity and Defamation: Users must not upload or import computer data containing images of others that have been created, edited, or modified through electronic means in a manner likely to cause loss of reputation, contempt, hatred, or embarrassment to those individuals.

2.10 Session Termination: Upon completing internet-related tasks, users must close the web browser immediately to prevent unauthorized access by others.

Section 15: Electronic Mail (E-mail) Usage Guidelines

1. Objectives

1.1 To ensure that the transmission of information via the Company's electronic mail system effectively supports the operations and administration of Thai Rubber Latex Group Public Company Limited and its subsidiaries, ensuring accuracy, convenience, speed, and overall efficiency.

1.2 To establish a standardized framework for e-mail communication among personnel and departments that remains within the boundaries of applicable laws, regulations, orders, and Company bylaws.

2. E-mail Operational Guidelines

2.1 Access Management: Administrators shall assign e-mail access rights appropriate to the user's role and responsibilities. These rights must be reviewed regularly, particularly in the event of resignation or internal job rotation.

2.2 Identity Verification: Administrators must establish unique user accounts and initial passwords for new users to ensure proper identity verification within the Company's e-mail system.

2.3 Initial Login Protocols: New users will receive a default password for their first access. Upon the initial login, the system must mandate an immediate password change.

2.4 Credential Masking: During the password entry process, characters must not be visible on the screen and must be replaced by masking symbols such as 'x' or '*' for each character typed.

2.5 Account Lockout Policy: Administrators should configure the system to limit unsuccessful login attempts to a maximum of three (3) consecutive times.

2.6 Session Timeout: The e-mail system should be configured to automatically log out or terminate a session after a designated period of inactivity (e.g., 15 minutes). Users must re-authenticate with their username and password to resume access.

2.7 Automated Credentials: Users must not enable "Save Password" or auto-fill features for e-mail credentials on any device.

2.8 Password Rotation: Users are required to strictly adhere to password rotation policies, with a recommended change interval of every 3 to 6 months.

2.9 Professional Conduct and Ethics: Users must exercise caution when using electronic mail to prevent reputational damage to the Company or violations of the rights of others. Prohibited activities include sending unlawful, immoral, or harassing content. Furthermore, users must not utilize the corporate e-mail network for personal business gain or permit others to do so.

Section 16: E-mail Terms of Use and Disclaimer

1. Objectives

1.1 To ensure that the Company's electronic mail communication effectively supports operational tasks with accuracy, convenience, speed, and efficiency.

1.2 To establish professional communication standards for all personnel and departments within the framework of applicable laws, regulations, orders, bylaws, and the Information Security Measures of Thai Rubber Latex Group Public Company Limited and its subsidiaries.

2. Compliance with Legal Frameworks

Users of the Company's e-mail system must strictly adhere to all applicable laws and regulations, including but not limited to:

- Cybersecurity Act B.E. 2562 (2019)
- Computer-Related Crime Act (No. 2) B.E. 2560 (2017)
- Electronic Transactions Act (No. 4) B.E. 2562 (2019)
- Computer Usage Regulations as defined by the Company.

3. Terms and Conditions of Service

3.1 Corporate Interest: All departments and individuals utilizing the Company's e-mail service must do so solely for the benefit of the Company.

3.2 Commercial Prohibition: Use of the e-mail system for personal business ventures or private gain is strictly prohibited.

3.3 Institutional Respect: The service must not be used to disseminate, reference, or insult the National, Religious, or Monarchical institutions, or engage in any act that causes damage to these institutions.

3.4 Criminal Activity: Use of the e-mail system for cybercrime or any act violating laws, orders, corporate by laws, or confidentiality measures is strictly prohibited.

3.5 Inappropriate Content: Users must not disseminate improper information, images, audio, or text that could bring disrepute to others.

3.6 Personal Opinions: Use of the Company's e-mail address to express personal opinions that negatively impact or damage the reputation of individuals or the Company is prohibited.

3.7 Impersonation: Forging an e-mail address or impersonating another individual is strictly prohibited.

3.8 System Resource Abuse: Activities that disrupt system resources are prohibited, including:
(1) Creating or forwarding Chain Mail.
(2) Sending mass unsolicited e-mail (Spam Mail).
(3) Sending continuous disruptive e-mail (Letter Bombing).
(4) Distributing computer viruses via e-mail.

3.9 Server Integrity: Users must refrain from any action that may cause degradation or damage to the Company's e-mail server systems.

3.10 Credential Secrecy**:** Users must maintain the absolute confidentiality of their personal or departmental passwords.

3.11 Confidential Data: Transmission of the Company's confidential information to unrelated third parties or unauthorized departments is strictly prohibited.

3.12 Encryption Requirements: Any necessary transmission of confidential information to external parties must be encrypted in accordance with the Company's security standards.

3.13 Credential Security: If there is any suspicion of credential leakage (E-mail Address or Password), users must change their password immediately. Passwords must meet "Strong Password" criteria to ensure they are difficult to guess.

3.14 User Education: All users must study the user manual, operational regulations, and terms of use to ensure the correct and safe operation of the e-mail system.

3.15 Right to Suspend Service: In the event of complaints, legal requests, or discovery of unlawful acts, the Company reserves the right to temporarily suspend or terminate service to investigate the cause and extent of the incident.

3.16 User Liability: Any activity related to the dissemination of content via e-mail or user-hosted pages is the sole responsibility of the user. The IT Department shall not be held liable for any such actions.

Section 17: Physical and Environmental Security

1. Objective

To establish measures for controlling and protecting access to information technology (IT) service areas. This policy prioritizes the importance of IT equipment and data, which are valuable assets requiring confidentiality. These measures apply to all service users and external parties involved in the utilization of the Company's IT systems.

2. Physical and Environmental Security Guidelines

2.1 Area Classification: The AI/IT Department at the Head Office is responsible for clearly defining and designating IT service areas. Floor plans showing these areas must be published. Areas are classified into working spaces, IT/network equipment storage and installation areas, and wireless network coverage zones.

2.2 Access Rights: The AI/IT Department at the Head Office determines the access privileges for each IT service area.

2.3 Entry/Exit Control: The AI/IT Department at the Head Office establishes measures to monitor and control the entry and exit of all personnel in IT service areas.

2.4 External Equipment: Any external party bringing a computer or network equipment for use within the internal network must register via the "Equipment Authorization Form" and obtain a signature from an authorized supervisor.

3. Asset Control and Computer Usage (Clear Desk and Clear Screen Policy)

Information assets, such as documents, storage media, and computers, must be protected from unauthorized access. Users are required to log out information systems whenever the equipment is unattended.

3.1 Physical Security Perimeter:

3.1.1 Maintain a physical environment that prevents unauthorized external intrusion.

3.1.2 Conduct physical risk assessments and establish risk mitigation measures.

3.1.3 Office walls or areas housing IT systems should be constructed as solid, opaque structures.

3.1.4 Entrance doors and access points must be designed to resist physical intrusion.

3.1.5 Server room doors must be equipped with locking systems to prevent unauthorized entry.

3.1.6 IT personnel must ensure all doors and windows are locked after working hours.

3.1.7 Security systems, including security guards and CCTV surveillance, must be implemented to monitor external access.

3.1.8 Fire exit doors and adjacent walls must be constructed with sufficient heat resistance.
3.1.9 Company IT infrastructure areas must be physically separated from areas managed by external service providers.

3.2 Public Access, Delivery, and Loading Areas:
3.2.1 Restrict access to delivery and loading zones to prevent unauthorized entry to internal areas.
3.2.2 Limit personnel permitted in delivery and loading zones.
3.2.3 Isolate delivery areas from other internal office spaces to avoid accidental or intentional unauthorized access.
3.2.4 Inspect hazardous materials or production factors before transferring them to operational areas.
3.2.5 Register and audit all products delivered by vendors or external providers in accordance with the Company's procurement and asset management procedures.

3.3 Equipment Siting and Protection:
3.3.1 Site equipment in areas that minimize unnecessary access by general office staff.
3.3.2 Position IT systems to prevent unauthorized viewing of sensitive data (e.g., angling screens away from customer/visitor view).
3.3.3 Store critical equipment in a separate, secured area specifically for high-security assets.
3.3.4 Food, drinks, and smoking are strictly prohibited in computer control rooms.
3.3.5 Regularly monitor environmental conditions in computer rooms, such as maintaining normal temperature levels, to prevent equipment damage.
3.3.6 Implement measures to protect electrical equipment from power fluctuations or surges.

3.4 Supporting Utilities:
3.4.1 Ensure adequate supporting utilities (e.g., Air Conditioning, Ventilation, and Uninterruptible Power Supply (UPS)). These systems must be tested regularly to ensure operational continuity.
3.4.2 Use UPS systems to protect against power instability. Test these systems according to the manufacturer's recommendations. Maintenance Contracts Security for Workspaces and Other Assets:
3.5.1 Every staff member is responsible for protecting Company assets.
3.5.2 Users must log out of systems immediately when leaving a workstation unattended.
3.5.3 Store sensitive documents in secure, locked cabinets. Do not leave sensitive documents on desks (Clean Desk Policy).
3.5.4 Secure fax machines and mail receiving areas when not in use.
3.5.5 Prevent unauthorized use of computer equipment (e.g., PCs, cameras, printers, copiers, scanners).
3.5.6 Remove printed documents from printers immediately upon completion.

Section 18: Cloud System Security Controls

1. Objective

To establish security guidelines for the utilization of Cloud Systems within Thai Rubber Latex Group Public Company Limited. This policy aims to ensure data integrity and security in alignment with ISO/IEC 27001 standards and relevant legal frameworks, focusing on the protection of critical corporate, customer, and partner information.

2. Scope

This policy covers all forms of Cloud Service utilization:

2.1 SaaS (Software as a Service): Software services delivered via the cloud where users access applications over the internet without local installation. The provider manages the infrastructure, software, and updates. Examples include Corporate E-mail and Microsoft Office 365.

2.2 PaaS (Platform as a Service): A cloud service providing a ready-to-use platform for developers to build, test, and deploy applications without managing underlying infrastructure such as operating systems, hardware, or databases.

2.3 IaaS (Infrastructure as a Service): On-demand delivery of IT infrastructure resources, including servers (virtual or physical), storage, and networking. Users manage the operating systems and applications while paying only for actual resource consumption.

3. Cloud System Operational Guidelines

3.1 Identity & Access Management (IAM):

- Implement Role-Based Access Control (RBAC) to define user privileges according to job functions.
- Enforce Multi-Factor Authentication (MFA) for all system access.
- Maintain comprehensive Audit Logging to monitor and record all system access activities.

3.2 Data Protection:

- Implement Encryption for data both in transit and at rest.
- Establish Backup & Disaster Recovery plans to ensure business continuity in the event of data loss.
- Ensure Data Segregation in multi-tenant environments to isolate customer or departmental data.

3.3 Risk & Vendor Management:

- Conduct regular security assessments and audits of Cloud Service Providers.
- Define risk levels based on data sensitivity and usage requirements.
- Establish formal Service Level Agreements (SLA) and Security Agreements with providers.

3.4 System & Network Security:

- Deploy threat prevention measures, including Firewalls, IDS/IPS, and Anti-Malware.
- Implement network segmentation within the cloud environment and strictly control external access.
- Perform regular Vulnerability Scanning and system patching.

3.5 Incident Response:

- Maintain a formal Incident Response Plan and notification protocols for security events.
- Log and analyze security incidents to prevent recurrence.
- Report significant security incidents to relevant stakeholders in accordance with corporate policy.

3.6 Compliance & Governance:

- Adhere to data protection laws, including PDPA and GDPR.
- Align operations with international security standards such as ISO/IEC 27001 and the CSA STAR framework.
- Communicate clear cloud usage policies and guidelines to all authorized users.

Section 19: Artificial Intelligence (AI) Usage Control

1. Objective

To establish guidelines for the ethical, transparent, and secure utilization of Artificial Intelligence (AI). This policy aligns with ISO/IEC 27001 standards as well as legal frameworks such as PDPA and GDPR. The primary goal is to support organizational productivity while ensuring that information security and privacy rights are not compromised.

2. Scope

This policy covers all types of AI applications utilized within the organization that are officially provided and authorized by the Company only.

3. AI System Operational Guidelines

3.1 Input Data Security:

- Clearly define data classifications permitted for AI input and strictly prohibit unauthorized data (e.g., personally identifiable information (PII) and corporate trade secrets).
- Implement Anonymization or Pseudonymization of data before submission to AI systems.
- Verify user permissions prior to accessing training data or operational datasets.

3.2 Access Control:

- Adhere to the Principle of Least Privilege, granting only the minimum necessary access required for each task.
- Establish Role-Based Access Control (RBAC) specifically for AI developers, end-users, and system administrators.
- Enforce Multi-Factor Authentication (MFA) for accessing sensitive datasets or core AI systems.

3.3 Data Encryption:

- Enforce robust encryption for data both in-transit and at-rest.
- Utilize secure communication protocols, such as HTTPS/TLS.
- Implement a rigorous Key Management system to secure cryptographic keys.

3.4 Output Data Security:

- Implement validation measures to prevent AI from inadvertently displaying or disclosing confidential information.
- Utilize Data Loss Prevention (DLP) systems to detect and prevent data leakage through AI-generated outputs.
- Maintain Logging & Monitoring protocols to audit AI outputs and assess potential security risks.

3.5 Prevention of AI-Specific Threats:

- Establish defenses against Prompt Injection and Data Poisoning that could cause the AI to malfunction or reveal classified data.
- Monitor for Model Inversion Attacks, where malicious actors attempt to reconstruct original training data from the AI model.
- Ensure regular security updates and patching of the AI platform and its underlying components.

3.6 Governance & Compliance:

- Strictly comply with relevant laws and standards, including PDPA, GDPR, and ISO/IEC 27001.
- Maintain a clear and comprehensive AI Usage Policy focused on information security and ethical standards.
- Conduct regular risk assessments and reviews of AI systems to ensure continued safety and compliance.

Roles, Responsibilities, and Authorities

The segregation of duties aims to mitigate infrastructure risks. A clear distinction must be maintained between system development personnel and system administration personnel (who manage the production environment). Roles and responsibilities within the AI/IT Department are defined in writing, including the designation of backup personnel for critical functions to ensure operational continuity.

1. Policy Level (Governance)

Responsible for policy formulation, providing recommendations, and overseeing compliance. This level is accountable for risks or damage arising from system or data failures caused by negligence or non-compliance with security policies.

- Director
- AI/IT Manager

2. Operational Level

- AI/IT Manager and Teams

2.1 Monitoring and Risk Management: Overseeing operations, reviewing plans, and monitoring databases and IT security risks.

2.2 Database and Information Security Control: Ensuring the security of information systems and databases.

- Key Duties:
  - Comply with Access Control policies (Section 2 and Section 7).
  - Coordinate disaster recovery and contingency plans for database security.

2.3 Infrastructure and Network Maintenance**:** Managing servers, network rooms, and data backups.

- Key Duties:
  - Comply with Network Access policies (Section 5).
  - Control server room access and maintain server/network hardware.
  - Monitor system logs, perform backups/recoveries, and prevent unauthorized hacking attempts.

2.4 Internet Security

2.5 General Security

Information Security Incident Response Operations

1. Intrusion Prevention System (Daily Plan)

Review logs and reports to identify:

- Attack frequency and most common attack types.
- Predictable patterns in attack behavior.
- Severity levels and attacker IP addresses.

2. Firewall Management

- Review firewall rules at least once a month.
- Analyze log files for blocked packets, identifying the nature and origin (IP) of high-frequency blocks.
- Report detected attacks or security breaches to the AI/IT Manager for immediate action.

3. Internet Threat & Malware Protection

Daily/Weekly/Monthly monitoring of viruses, worms, Trojans, and spyware:

- Identify high-frequency malware types and their sources/destinations.
- Monitor for outbound malware transmission from the internal network.
- Quarantine and remediate infected devices immediately by disconnecting them from the network.

Emergency Contact Directory

1. AI/IT Department

- AI/IT Manager
- Head of Data Analysis & Ops
- Head of App Development
- IT Officer

2. Executive Data Custodians

- Director
- AI/IT Manager

3. Occupational Safety, Health and Environment Committee

4. Building Security / Physical Emergencies

- Security Guard