STECON Group Public Company Limited and subsidiaries company have implemented an information technology system to facilitate and enhance operational with effectiveness. These guidelines have been established to ensure that the proper use of the information technology system, including the efficient management of information technology resources, security system, and prevent from any potential issues arising from improper usage. Furthermore, cyber threat prevention has been implemented to protect against various threats that may impact the information technology system.

STECON Group Public Company Limited and subsidiaries company have established the security of information technology systems policy, as follows

Scope of the information technology system security policy

Following are the objectives of the information technology system security policy for STECON Group Public Company Limited and subsidiaries company

1. To ensure the stable security of the information technology system.
2. To set up practice procedures for the security of the information technology system by administrators, users and relevant persons.
3. To educate the importance of cyber security awareness.
4. To facilitate the assessment and evaluation of risks related to the security of the information technology system.

The information technology system security policy of STECON Group Public Company Limited and subsidiaries company consists with the following sections

Section 1: Definitions

Section 2: Authority and responsibilities

Section 3: Information technology system security

Section 4: Access rights and security for information technology systems

Section 5: Information protection policy

Section 6: Security procedures for information technology systems

Section 7: Regulations of internet and email usage

Section 8: Information technology system management and prevention policy

Section 9: Information technology system protection and recovery policy

Section 10: Information technology network administrator guidelines

Section 11: Penalties and enforcement

Definitions

The definitions in the information technology system security policy as follows

"Company" refers to STECON Group Public Company Limited and subsidiaries company.

"Information technology system" refers to computer hardware, such as servers, workstation computers, desktop computers, laptops, smart devices, tablets, printers, scanners, etc., or computer software, such as virtual machines, databases, commercial programs, and in-house programs that developed by the information technology department. It also includes the information technology network system.

"Information technology network system" refers to the communication or transmission of data between internal and external parties, such as the internet, routers, firewalls, network switching, wired networks, wireless networks, and wireless access points.

"Group chief executive officer/President" refers to the group chief executive officer/President of STECON Group Public Company Limited.

"Employees" refers to the employees and staff of the company, including individuals assigned by the company to perform tasks under employment contract, agreement, or purchase order.

"Information" refers to any material that can be represented meaning or factual content, regardless of how the communication is made, its form, or the method used to make it visible. This includes documents, files, reports, books, diagrams, maps, drawings, photographs, images, animations, videos, audio recordings, or recordings made using computers.

"Information technology system administrator" refers to the information technology manager, who is appointed by the Group chief executive officer/President and is responsible for maintain the security of the information technology system and can access to information technology programs for managing network database. This permission may be delegated to the information technology staff to act on behalf of as appropriate.

"Confidential Information" refers to information stored in the form of data or recorded content that is classified and restricted based on the level of importance, with access limited to those who need to know. This also includes recorded media, passwords, user accounts, and documents containing such information.

Authority and responsibilities

1. Information technology manager's responsibilities
    1.1 Supervise and provide guidance to the information technology system administrators.
    1.2 Advice and recommendations to information technology system administrators.
    1.3 Provide suggestions to the group chief executive officer/president regarding policies and measures related to the security of the information technology system.
    1.4 Report operational performance to the group chief executive officer/president.
    1.5 Carry out additional duties as assigned by the group chief executive officer/president.
    1.6 Maintain security and assess risks of the information technology system.

2. Information technology network administrator's responsibilities
    2.1 Manage access of the information technology network system.
    2.2 Maintain the infrastructure and equipment related to the information technology network system.
    2.3 Set up user accounts for accessing the information technology network system.
    2.4 Maintain security and assess risks of the information technology network system.

3. Program developer's responsibilities
    3.1 Develop programs as assigned.
    3.2 Prepare test data to ensure the accuracy of program functionality.
    3.3 Maintain, update, and improve developed programs to ensure programs are up-to-date and ready to use at any time.
    3.4 Ensure all programs are secured by perform risks assessment.

4. Information technology service officer's responsibilities
    4.1 Control and manage the use of the company’s office computer equipment.
    4.2 Control and monitor the installation of all programs to align with the company’s objectives.

4.3 Handle information technology services such as maintenance, troubleshooting, updates, virus scanning, and providing user guidance.

4.4 Provide recommendations and encourage company employees to follow proper procedures for accessing the information technology system.

4.5 Make an inventory of equipment, usage status, and the utilization of computer equipment.

4.6 Minimize risks of data leakage when computer equipment is damaged or retired by properly destroying data to prevent recovery. This includes establishing asset disposal methods to maximize value while considering environmental impacts, such as recycling.

Information technology system security

- Data center room

The data center room is used for company's information technology systems, which include the following components

1. Server systems.
2. Security systems for the information technology network.
3. Network connectivity systems for the information technology network.
4. Uninterruptible power supply systems for all equipment within the data center.
5. Temperature control systems to maintain optimal conditions for all equipment in the data center.
6. Access control systems for the data center.
7. Fire suppression systems suitable for all equipment within the data center.
8. Management systems for all company computer equipment.
9. Internal data backup systems and backup systems to offsite data center.
10. Closed-circuit television (CCTV) systems within the data center.

Therefore, the data center room is an important area of the company, it is requiring strictly security with the following regulation

1. The data center room has a single entrance that always remains closed and is equipped with appropriate security systems.
2. Access to the data center room is restricted to authorized personnel only. Authorized individuals include the information technology manager, designated operators, or external contractors who are responsible for system installation, repairs, or maintenance. Designated personnel must always supervise and monitor the work of external parties while they are in the data center.

3. Entry to the data center room must be authenticated through access control devices, which must be capable of saving history all entry records.
4. The information technology manager is responsible for regularly reviewing access to the data center by monthly basis.
5. The data center room must maintain appropriate temperature control systems for all equipment, with annual maintenance of the temperature control system.
6. The data center room must have a backup temperature control system to be used in case the primary system fails, and temperature monitoring must be accessible remotely at any time.
7. The data center room must be equipped with a backup power supply and surge protection systems suitable for all equipment, with regular testing of the backup power supply conducted annually.
8. The data center room must have an adequate fire suppression system, with annual testing of the fire suppression system.
9. The data center room must have a surveillance camera system that records the activities of individuals entering the data center room. The recorded footage must be stored securely, and remote viewing of the surveillance cameras must be available at any time.
10. Access to the data center is strictly prohibited for individuals who are not authorized or involved in its operations.

- **Personal computer usage guidelines**

  Employees who utilize company computers must adhere to the following guidelines:

  1. Employees must use only their own user accounts to access the company's information technology systems.
  2. Employees are responsible for maintenance company computers and peripheral equipment in good condition, ensuring they are functional, undamaged, and used efficiently.
  3. Important data must be securely stored and safeguarded to prevent unauthorized access.
  4. Additional software installation required by users must be approved by the respective department. The information technology department is authorized to perform software installations only.
  5. Employees are prohibited from installing or using software that infringes intellectual property rights on company computers. Similarly, employees are forbidden from using pirated software on personal computers within the company's network or in conjunction with the company's email system. In the event of a legal complaint regarding intellectual property infringement, the violator will be personally liable for the violation.

6. Employees are not permitted to modify, alter, remove, or add any hardware or software to the company's information technology systems without approval. If necessary, such actions must be carried out by the information technology department.
7. External individuals are not allowed to use the company's computer equipment. In cases of necessity, a request must be made to the information technology department for assistance with such usage.

Access rights and security for Information technology systems

Employees granted access to the company's information technology system must adhere to the following guidelines

- User account policy for employees

User accounts are created based on requests approved by the department head. Access levels and permissions are granted according to the necessity of the job, with discretion held by the information technology manager, who may adjust access rights to align with the business needs. Accounts grant access to company resources, including the information technology network, databases, shared resources, remote access, and email configuration.

- User account policy for information technology administrators

All configuration changes and additional access requests must be approved by the information technology manager. Any modifications to the system settings require authorization from either the information technology manager or system administrators.

- General guidelines

1. Employees must use information technology resources responsibly and efficiently.
2. Communication within the system, particularly through email, should be professional and follow international standards. Mass emails should only be used for work-related purposes.
3. Employees must ensure the security of the information technology network, never allowing others to use their accounts.

- Personal passwords

Employees must adhere to the following guidelines regarding personal password usage

1. Passwords must be at least 6 characters long, combining upper and lowercase letters, numbers, and symbols. Avoid easily guessed passwords such as names, family names, related names, phone numbers, or common phrases. Such as, P@ssw0rd, Abc!23, !L0veyou, Le!me1n.
2. When sharing files, users must manually enter their passwords. Automatic password saving features are not permitted.
3. Employees must not disclose their passwords or store them in easily accessible locations.
4. Passwords must be changed every 90 days.
5. Passwords for ERP and HR system must be changed every 60 days.
6. Employees can reset their passwords through self-service tools or by contacting the information technology department.
7. When an employee's name, position, or department changes, the information technology department must update their account. Accounts are deactivated upon resignation.

- **Remote information technology system access**

Access to information technology systems from outside the office must be granted only to individuals who have a legitimate need for such access and who have received approval from their respective departments and the information technology manager. The following guidelines apply

1. Remote access requires approval from the department head and information technology manager, and employees must connect using a company-installed Virtual Private Network, VPN.
2. Employees must use their personal credentials for remote access authentication.
3. After completing tasks, users must immediately disconnect from the VPN.
4. When using public networks, employees must verify the network's security, ensure their antivirus software is still active, and avoid downloading untrusted files. If any system anomalies occur, employees must shut down the computer and submit it to information technology for inspection.

Information protection policy

To use company data and information technology resources must be conducted by employees using their own account name and personal password for identity verification. Employees must not use the company's information technology resources for the following purposes

1. Engaging in illegal activities or actions that may cause harm to others.
2. Engaging in actions that are against public order or morality.
3. For commercial purposes.

4. Disclosing confidential information obtained through work, whether it pertains to the company or external parties.
5. Actions that violate the intellectual property of the organization or others.
6. Accessing information about others without authorization from the owner or the rightful holder of that information.
7. Receiving or sending information that may cause or potentially cause harm to the company, such as chain letters, mass emails, or forwarding information from external parties that violate laws or rights to other employees or individuals.
8. Disrupting the normal use of the company's information technology network or obstructing its functionality for employees.
9. Expressing personal opinions regarding the company's operations on social media in a manner that could lead to misunderstanding or misrepresentation of the facts.
10. Any other actions that may conflict with the company's interests, lead to conflicts, or cause damage to the company.

Security procedures for information technology systems

To ensure the security of the company's information technology systems, employees are required to follow the procedures outlined below

1. Do not install or use software that infringes on the intellectual property rights of others.
2. Do not install or use software capable of monitoring information on the IT network, unless authorized by the information technology manager.
3. Do not install or use software that allows others to access your personal computer or other systems on the company's information technology network, unless approved by the information technology manager.
4. Shut down your computer at the end of each workday, unless it is a server providing continuous services.
5. Always scan data received from external sources using antivirus software as specified by the information technology department. If a virus is detected, immediately destroy the virus or the infected data, or notify the information technology department to handle the situation.
6. When accessing the company's network from an external location, use only software specified by the information technology department.
7. Cooperate with the information technology department in conducting security audits of your personal computer and adhere to their instructions.

8. Handle and maintain personal computers and information technology networks carefully to ensure they can be operated at any time.
9. Safeguard and secure company data.
10. When sending sensitive company information, ensure the highest level of data security.
11. Caution when printing or duplicating documents, maintaining confidentiality, and securely storing sensitive information.
12. Before sending a computer or storage device for repair to the information technology department, backup all data and store it securely is required to prevent data loss.
13. Return all company property related to information technology systems, including computers, data, and copies of data, before the end of employment.
14. Do not enter the data center room without prior authorization.

Regulations for internet and email usage

To ensure safe use of the internet and email, employees must adhere to the following guidelines

- Internet
  1. Access the internet through your personal account only.
  2. Utilize the Internet strictly for work-related purposes.
  3. Do not download any software, games, images, or other data that are unrelated to work.
  4. Avoid accessing or viewing images, videos, or content of a pornographic nature or that violates public morality.
  5. Do not play online games or use any game-related services.
  6. Refrain from sending images, videos, messages, or any form of content that may harm the company's reputation, esteemed institutions, religions, organizations, or third parties.
- Email
  1. Use your own personal email account for company-related work only.
  2. Utilize the company email solely for work-related purposes.
  3. Do not disclose your personal email password to anyone.
  4. Refrain from sending chain emails or mass emails that are not work-related.
  5. Always scan email attachments for viruses before opening them.

Information technology system management and prevention policy

Information technology system security is crucial for the company to ensure proper and efficient use of information systems, minimize risks in operations, and manage the network effectively. The following rules are established to ensure the security and efficiency of IT systems

- **Data backup**

The primary function of data backup is to create copies of existing data to protect against data loss from malicious attacks and ensure data recovery when needed. The guidelines are as follows

1. The person who is assigned and authorized by their supervisor may perform data backups and store backup data in a secure location.
2. The person in charge must backup data and store it according to the established data preservation guidelines.
3. Backup storage should be located both within the company and outside the company. For external storage, the company's headquarters should use a backup data center.
4. Written notification is required for moving or changing the storage location of backup data, and approval from the supervisor must be obtained beforehand.
5. The responsible personnel must ensure the immediate availability of backup media from the storage location and be able to recover the system quickly if an unexpected information technology system failure occurs.

- **Information technology network status reporting**

The purpose of reporting the information technology network status includes the following

1. To monitor and maintain information technology system security by reviewing usage of the network.
2. Information technology network administrators must keep records of internet and email traffic, and data from other systems by example system errors, backup and recovery processes, anti-virus, wireless network data.
3. Administrators must verify for unauthorized access, password guessing, and shared data misuse.
4. Regular maintenance and monitoring of the data center room and backup computer systems are required to ensure continuous normal operation.
5. Information technology network administrators must report the network's status during information technology department meetings to inform staff of risks and threats and collaborate on solutions and preventive measures.

- **Intrusion prevention and virus protection**

The company provides proper information technology system security equipment. Following are the responsibilities of information technology network administrators

1. Install a firewall to prevent unauthorized access to the company's information technology network.
2. Regularly update the anti-virus software on all computers to maintain up-to-date protection.
3. Scan computer viruses for all incoming and outgoing emails.
4. Mitigating computer operating system vulnerabilities by frequently updates security patches.
5. Disconnect infected computers from the network to prevent the spread of computer viruses and proceed with virus elimination.

- **Computer equipment security and service control**

1. Set personal passwords to prevent data leakage or damage.
2. The information technology department is responsible for managing the company's information technology equipment, ensuring its appropriateness for each department's requirements.
3. Purchasing of Information technology equipment must follow the company's procurement process, with approval from the supervisor.
4. The information technology department must register all received assets by assigning a machine number and recording necessary details for each equipment type.
5. Moving information technology equipment between locations must be approved by the supervisor.
6. The information technology department must support and maintain information technology equipment efficiently and store maintenance records for every service.
7. To enhance data security and prevent data loss during remote services from the information technology department. Getting consent from employees is required before starting the services.
8. The disposal of information technology equipment must be authorized by the CEO or the Managing Director.
9. Employees who install or use software that infringes intellectual property rights on company computers, or on their personal devices, will be held personally responsible for legal violations.

- **Standard of data security and software development**

Developing programs must be secure and resistant to attacks. Programs should be designed to prevent attacks commonly used by malicious actors, such as Denial of Service (DoS), Spoofing, Malware, Ransomware, and Phishing.

The following guidelines apply to secure software development

1. Perform vulnerability assessments.

2. Implement authentication and identity verification.
3. Define access permissions to data.
4. Record logs of access programs and misuse of attempts password.
5. Test database attacks by SQL injection.
6. Set limits on incorrect password attempts or use multi-factor authentication to prevent denial of service attacks.
7. Encrypt data during transmission to prevent spoofing attacks.

The following guidelines apply for international standards software development:

1. Developers must adhere to standard and generally accepted programming methods, providing the necessary security information, source code, development documentation, user manuals, and any relevant data.
2. Supervisors determine the qualifications of users and assign access rights accordingly.
3. Programs must test before release to users, and users must verify the program's correctness and sign off upon receipt.
4. Development on a central database must be performed on a test database to avoid errors and maintain data security.
5. Network-based program installations are handled by information technology network administrators, while specific installations are performed by the information technology service section.
6. In cases when developers need to modify network-based programs, network administrators will grant access on a case-by-case basis and monitor the developer's work until completion.

Information technology system protection and recovery policy

To comply with the security and rapid recovery of information technology systems in accordance with international standards, Prevention of any errors or any damages that may arise due to various threats are required.

For the headquarters' information technology systems, the information technology department must backup all data and systems to a disaster recovery site. This ensures data integrity and system availability in the event of a failure or disaster. Procedure for recovery and recovery method for critical systems are required. The recovery methods must be tested regularly to ensure they can effectively restore essential systems and data, minimizing significant impacts on the company's operations. Regular testing of data recovery and system recovery, particularly for critical systems, is required. This testing ensures that recovery procedures are reliable and can prevent substantial disruption to business activities. Data and system backups, as well as recovery

methods, must comply with the company's data backup and recovery guidelines to maintain continuity and security across the organization.

Information technology network administrator guidelines

1. The information technology network administrator is responsible for maintaining and updating the information technology network to ensure it always functions optimally. This includes assessing new threats and monitoring the network's usage to ensure compliance with this policy. If any employees are suspected of violating the usage guidelines, the administrator must promptly report the incident to the relevant supervisor.
2. If any incident is deemed to potentially harm the company, the information technology network administrator has the authority to immediately suspend the employee's access to the information technology network.
3. The information technology network administrator must provide feedback and observations to the information technology manager to enhance the efficiency and management of the information technology network.
4. The information technology network administrator is responsible for installing information technology equipment and related systems, as well as ensuring their regular maintenance to maintain optimal functionality.
5. In case of resignation of the information technology network administrator or designated employee. All assets must return to the information technology manager to ensure data and network security.

Penalties and enforcement

1. Employees who violate this policy will receive disciplinary and legal action in accordance with the company's regulations and guidelines.
2. The information technology department is responsible for strictly monitoring compliance with this policy.
3. This policy has been approved by the board of directors in meeting No. 2/2567 on February 27, 2024, and shall take effect from February 27, 2024, onward.

Effective date on February 27, 2024

Sign .....

(Mr. Vallop Rungkijvorasathien)

Chairman of the Board of Directors

STECON Group Public Company Limited