Information Technology Security Policy
Proud Real Estate Public Company Limited

Proud Real Estate Public Company Limited uses information technology systems to support its operations and provide services to users both within and outside the organisation. To ensure that the use of information technology systems is appropriate, efficient and secure, and that operations can continue without interruption, as well as to prevent problems that may arise from improper use or various threats and thereby reduce risks that may affect the Company's operations, the Company has established the Information Technology Systems Security Policy with the following objectives:

1. To establish policies and guidelines for directors, executives, employees of the Company and other relevant persons to follow correctly and in compliance with the law on computer-related offences and other relevant laws.

2. To ensure that the Company's information technology systems meet information security standards, with access restricted to authorised persons (Confidentiality), information maintained accurately and completely (Integrity), and systems available for use when required (Availability).

3. To communicate the Information Technology Systems Security Policy to directors, executives and employees, and to publish the Policy on the Company's website so that relevant external parties are informed of and strictly comply with the Policy.

Definitions

"Company" means Proud Real Estate Public Company Limited.

"Subsidiary" means a company with any of the following characteristics:

1. a company over which the Company has control;
2. a company over which the company referred to in (1) has control, and so on through successive levels of control, beginning with the company referred to in (1).

"Group" means Proud Real Estate Public Company Limited and its subsidiaries.

"Controlling Power" means a relationship having any of the following characteristics:

(1) holding shares with voting rights in a company in excess of fifty per cent of the total voting rights of that company;

(2) having control over a majority of the voting rights at a shareholders' meeting of a company, whether directly or indirectly or for any reason;

(3) having control over the appointment or removal of at least one-half of all directors of a company, whether directly or indirectly.

"User" means a director, executive, employee or Related Person who uses the computer systems of the Group.

"Related Person" means a person or juristic person, whether a government agency, state enterprise or private organisation, with which the Group has a business relationship or conducts any transaction relating to finance or the assets of the Group, such as management, purchasing, sales or engagement.

"System Administrator" means an information technology officer.

"Personal Data" means information relating to an individual that enables that individual to be identified, whether directly or indirectly. This also covers sensitive personal data, such as information concerning race, ethnicity, political opinions, beliefs, religion or philosophy, sexual behaviour, criminal records, health, disability, trade union information, genetic data and biometric data, which the Company has collected for use in its business operations.

"Data Subject" means an executive, Officer, Customer or external person who performs work for the Company.

"Officer" means a person employed by the Company, whether paid on a daily or monthly basis, as well as an employee on probation.

"Customer" means a person who has entered into a reservation agreement for goods or services or a sale and purchase agreement for goods or services with the Company, as well as a person interested in entering into such a reservation agreement or sale and purchase agreement with the Company.

"Undesirable or Unexpected Security Situation" means an undesirable or unexpected security situation that may result in the Company's systems being compromised or attacked and information security being threatened.

"Office" means the Office of the Personal Data Protection Committee.

"Security Incident" means an identified occurrence involving the status of a service or network that indicates the possibility of a breach of a security policy, failure of protective measures, or a previously unknown event that may be related to security.

Guidelines

1. The Company shall establish a written information technology security policy that complies with applicable laws and internationally recognised information security standards.
2. Information and information technology systems, information technology equipment, premises and environments related to information technology, the development and maintenance of information technology systems, and other matters related to information technology shall be appropriately secured, with clearly defined access controls.
3. The Company shall establish a data backup system, a data recovery system and a backup system that can replace the primary information technology system in an emergency. The backup system shall be maintained in a state of readiness, and an emergency preparedness plan shall be established.
4. Information technology risks shall be regularly reviewed and assessed in accordance with the Company's Enterprise Risk Management Policy.
5. Security incidents shall be investigated and corrective action taken when they occur. Measures shall also be taken to prevent recurrence, and such incidents shall be clearly reported and documented.
6. The Company shall ensure that users are informed of the policies, guidelines, standards and regulations relating to information technology security. Users shall strictly observe and comply with them.

Section 1

Good Corporate Governance and Management of Enterprise IT (Governance of Enterprise IT)

Information technology governance aims to ensure that the Company can achieve its established objectives through the use of information technology as a supporting tool and can effectively manage risks arising from the use of information technology. It also aims to ensure that the technology used by the Company can support its strategies and achieve its business objectives. The Company shall therefore take the following actions:

1. Information Technology Security Policy (IT Security Policy)
    1. The Company shall establish a written Information Technology Security Policy and communicate it through the Company's communication channels to ensure proper understanding and compliance.
    2. The Company shall review the Information Technology Security Policy whenever any change occurs that affects the Company's policy.
2. Information Technology Risk Management (IT Risk Management)

    Information technology risk management shall be consistent with the Company's Corporate Risk Management Policy and shall cover the following matters:
    1. Roles and responsibilities for information technology risk management

        The IT Manager shall be responsible for assessing and establishing methods or guidelines for information technology to reduce or manage existing risks and shall submit them to executives for consideration in the management of information technology system risks.
    2. Identification of information technology-related risks (Information Technology Related Risk)
        - Risks arising from the use of computer programs on the Company's computers. Measures shall be taken to prevent the use or installation of unsafe or unwanted programs, such as programs downloaded from external sources that may contain malware or computer viruses, or the exploitation of vulnerabilities through connections to external networks to attack computers in use or other computers on the same network.
        - Risks arising from the use of the Company's computer network. The use of the internal network and the Internet shall be monitored and controlled. Systems shall be established to protect servers and client computers used by personnel from unauthorised access and external attacks, such as controls over Internet access, computer antivirus software and email filtering.
        - Personnel risks. Access rights to computer systems, network equipment and data shall be defined according to the rights granted to each person to prevent the modification or alteration of data.
    3. Risks shall be assessed in terms of the likelihood of occurrence and potential impact to prioritise risk management. Risks shall be classified into four categories as follows:
        - Technology risk, which may arise from attacks on computers and equipment.
        - Personnel risk, which may arise from inappropriate access rights management, resulting in access to information beyond assigned responsibilities and possible damage to information.
        - Risk arising from threats and emergencies, which may arise from disasters or natural events, as well as other situations such as power outages and protests.
        - Management risk, which may arise from operational policies that are not consistent with potential risks.

4. Methods or tools shall be established to manage risks and maintain them at a level acceptable to the Company. A Description of Risk table shall be prepared with details such as the risk topic, risk category, risk characteristics, risk factors and impacts. The likelihood of occurrence and severity of the risk impact shall be determined, and a Risk Map shall be prepared.
5. Information Technology Risk Indicators shall be established. The indicators shall be monitored and the results reported to the responsible persons to ensure that risks can be appropriately managed in a timely manner.

Section 2

Information Technology Systems Security (IT Security)

- Additional Guidelines on IT Security Policies and Measures (Information Security Policy)

Objective

To prevent violations of the Information Technology Systems Security Policy.

Guidelines

1. The Company's resources and computer networks shall not be used to commit illegal acts or acts contrary to public morals, such as creating websites to disseminate content that violates the law on computer-related offences.
2. Users shall not access a computer network or computer using another person's user account, whether or not permission has been obtained from the owner of that user account.
3. Users shall not use another user's account without permission.
4. Information belonging to other persons or organisations shall not be disclosed without permission from the owner of such information.
5. The resources and computer networks of the Group shall not be interfered with, obstructed or damaged in a manner that causes damage, such as by transmitting computer viruses or introducing programs that cause computers or network equipment to cease functioning (Denial of Service).
6. Users shall not intercept data on the Group's computer network.

- Information Technology Systems Security Organisation (Organization of Information Security)

Objective

To establish a framework for the management of information technology systems security within the Group.

Guidelines

1. Senior executives shall be responsible for overseeing security in accordance with the Group's Information Technology Systems Security Policy and guidelines.
2. The head of the information technology unit shall define and assign duties to personnel in the information technology department who are responsible for the Company's information systems to ensure security and control over operations in accordance with the Group's Information Technology Systems Security Policy and guidelines.

3. An information technology officer assigned as the Administrator responsible for a particular system shall be responsible for that system. The officer shall monitor and review system security during use (Security Logs Review), and records of such reviews shall be maintained at intervals determined by the head of the information technology unit. If an undesirable or unexpected security situation occurs, corrective action shall be taken and the incident shall be reported to the officer's supervisor.
4. Users and Related Persons shall be responsible for compliance with the Company's policies and guidelines on information technology systems security and shall not violate laws relating to computer-related offences.

- Human Resource Security

Objective

To ensure that users understand the policies, duties and responsibilities relating to the use of the Group's information technology systems.

Guidelines

1. The duties and responsibilities relating to information technology systems security shall be clearly defined in writing for relevant persons engaged to perform work and shall be consistent with the Company's Information Technology Systems Security Policy.
2. Users and Related Persons engaged to perform work shall be informed of the policies relating to the Company's information technology systems security.
3. To ensure that user account management is accurate and up to date, the Human Resources Department or relevant unit shall immediately notify information technology officers in the following cases:
   - resignation or termination of employment;
   - transfer to another unit.
4. Users and external organisations engaged by the Company to perform work shall be informed of the policies relating to information technology security.
5. Access to information in information technology systems shall be revoked immediately upon any change to or termination of employment or upon completion of a project.
6. An agreement shall be signed between personnel and the relevant unit under which the personnel agree not to disclose the Company's confidential information (Non-Disclosure Agreement: NDA). The agreement shall form part of the engagement of such personnel and shall remain binding both during the engagement and for at least one year after the engagement ends.
7. New personnel of the Company shall receive training on the Information Technology Security Policy as part of their orientation.

- Information Asset Management (Asset Management)
  - Control of Computer and Peripheral Equipment Use (Computer and Peripheral Access Control)

    Objective

    To ensure that users understand their duties and responsibilities in the use of computers and peripheral equipment, maintain such equipment in good working condition, and use it properly to protect the Company's information assets and ensure that they remain secure, accurate and available for use.

Guidelines

1. Users of computers and peripheral equipment of the Group shall be responsible for the assets (Asset) they use.
2. Computers and computer networks of the Group shall not be used for personal business, trade or services, or for any purpose unrelated to the Group's business.
3. Users shall not install or modify software or alter any components of the Group's computers or peripheral equipment without permission from their supervisor and the head of the information technology unit. Only the System Administrator may install, modify or change software. Users shall maintain computers and peripheral equipment in good working condition at all times.
4. Users shall not place or use computer equipment in areas exposed to heat, moisture or dust, and shall take precautions against impact.
5. Computer equipment of any kind shall not be used or placed near liquids, magnetic fields, high-voltage electricity or in environments with temperatures above 35 degrees Celsius.
6. Computer equipment shall be moved with care. Heavy objects shall not be placed on the equipment, and the equipment shall not be thrown.
7. Hard objects shall be kept away from computer screens, as contact may scratch or crack the screens. Computer screens should be cleaned as gently as possible and wiped in one direction. They shall not be wiped in a circular motion, as this may scratch the screens.
8. Users who resign or complete a project shall return all computers and peripheral equipment under their responsibility to the responsible unit in good working condition.
9. Computer equipment required for work outside the office shall be moved in accordance with the Company's requirements for taking Company assets outside the premises.
10. Users shall be responsible for preventing the loss of their computers and shall not leave them unattended in public places or areas where there is a risk of loss.

- Control of Computer Software Use (Software License Management)

  Objective

  To ensure that users are aware of their duties and responsibilities in the use of computers and their rights to use computer software, understand the proper use of licensed software, and strictly comply with the relevant guidelines in accordance with the law on computer-related offences and other relevant laws.

  Guidelines

  Requirements for System Administrators

  1. System Administrators shall be responsible for controlling and overseeing the use of computer software and allocating the use of computer software within the Company in accordance with the specified usage rights.
  2. System Administrators shall be responsible for installing and upgrading computer software for users at the scheduled time.
  3. System Administrators shall manage and revoke computer software usage rights immediately upon notification from the Company and/or the relevant unit of the cancellation and/or transfer of such usage rights.

Requirements for Users

1. Users shall not use the Group's computer software for any illegal purpose that may cause damage to the Group.
2. Software installed on the Group's computers shall be properly licensed in accordance with applicable laws. Users shall not copy or reproduce such software for use on their own computers or for distribution to external parties unrelated to the Group.
3. Users shall not copy, distribute or disseminate software that infringes copyright or program instructions created without permission, particularly for use as a tool to commit offences under the law on computer-related offences and other relevant laws.
4. Users shall not install software that is not permitted by law on the Group's computers. If any illegal software is detected on the Group's computers or any software currently used on the computer system, whether Licensed Software or Freeware, causes damage or an infringement, the user shall bear sole responsibility.
5. The installation and use, termination of use, transfer and return of computers and computer software for users shall be considered on a case-by-case basis. The authorised person shall consider and approve such actions in accordance with the specified conditions, and the System Administrator shall proceed in accordance with the approval granted at each stage.

- Control of Information Technology Assets and Computer System Access
  (Asset and Information System Control)

  Objective

  To ensure that users are aware of their duties and responsibilities and do not expose assets and information to the risk of access by persons without the relevant rights or authority.

  Guidelines

  Requirements for System Administrators

  1. System Administrators shall prepare and maintain an information asset register as preliminary information for the analysis, assessment and management of risks to information assets, as well as for controlling and overseeing the Group's assets.
  2. System Administrators shall conduct an inventory check of all types of assets every six months.
  3. System Administrators shall assess risks in accordance with the asset risk management guidelines whenever new assets are acquired or significant changes to assets occur.

  Requirements for Users

  1. Users shall log out immediately after completing their use of the system.
  2. Computers shall be protected through appropriate authentication before use.
  3. Important information of the relevant unit shall be stored and backed up in a secure location. User data shall be stored in the database of the relevant application within the Company's Data Center.
  4. Information may be stored in the Shared File (central drive) in a Folder in accordance with the access rights granted to the user.
  5. Computer equipment shall be switched off when it has not been in use for more than one hour or at the end of each working day, except for computers used as servers that provide services requiring

continuous 24-hour operation.

6. Users shall configure the Screen Saver on their computers to automatically lock the screen after the computer has been inactive for more than 10 minutes.
7. Users shall exercise care and safeguard the Group's assets under their use as if they were their own. If any loss occurs as a result of the user's negligence, the user shall be responsible for compensating for such loss.

- Email Control

Objective

To ensure that the receipt and transmission of information by email can support work operations and can be carried out properly, conveniently, promptly, responsively, efficiently and securely, in accordance with applicable laws, regulations, requirements and the Group's information security measures. The objective is also to ensure that users understand the importance of and are aware of problems arising from the use of email or Internet services. Users must understand the rules established by the System Administrator, refrain from infringing any rights or taking any action that may cause problems or violate the established rules, and strictly comply with the System Administrator's instructions.

Guidelines

1. Users of the Company's email service (Email Address) shall not use the Email Address to commit offences under the law on computer-related offences or other relevant laws.
2. Departments or personnel who use the Company's email service shall use email for the Company's business purposes.
3. Personnel shall be granted the right to use the email service. The System Administrator shall register email users based on the list of personnel notified by the Human Resources Department.
4. Users shall not use another person's Email Address for any purpose, whether to read, receive or send messages, unless consent has been obtained from the owner of the Email Address. The owner of the Email Address shall be responsible for the use of that Email Address.
5. Users shall not impersonate another sender or use another user's account.
6. When providing an Email Address to persons relevant to the Group's business, users shall use only the Company's Email Address. Other Email Addresses shall not be used, except where the Company's Email Address system is unavailable and prior approval has been obtained from the user's supervisor.
7. Email Addresses shall be used in an appropriate manner and shall not be used in any manner contrary to public morals. Users shall not incite, provoke or make disparaging statements, disseminate content unlawfully, or send personal opinions in a manner that may be regarded as the opinion of the Group or may cause damage to the Group.
8. The Company's Email Address shall not be used to disseminate information, messages, images or other media that are contrary to public morals or national security, violate the law, defame the monarchy, or affect the operations of the Group, or to disturb other users or persons related to the Group.
9. Users shall not use their Email Address for personal activities, such as conducting personal business or using online social networking services. If the Company finds that such activities have occurred, the owner of the Email Address shall be responsible for such activities.

10. Users shall not take any action that may cause problems in the use of system resources, such as creating chain mail, sending large volumes of email (Spam mail), sending repeated email messages (Letter bomb), or sending email to spread computer viruses.
11. Users shall not disclose the Group's confidential information, such as customer information or operating plans, to external persons or organisations that are not related to the Group's business.
12. In the event of a complaint, request or discovery of any unlawful activity, the Company reserves the right to temporarily cancel or suspend the service of the relevant user in order to investigate and determine the root cause without prior notice or permission.
13. If users find any inappropriate action or illegal activity within the Company, they shall notify the System Administrator of the Information Technology Department.
14. Any dissemination through an Email Address or the homepage of a user shall be solely the responsibility of that user. The System Administrator and the Company shall have no involvement in such action.

- Control of Access to Data and Information Systems (Access Control)

  Objective

  To establish measures for Internet use through the Company's network to ensure efficiency and security, and to ensure that users are aware of the use of websites through the Company's network.

  Guidelines

  1. The Information Technology Department shall establish network connection routes for Internet access through security systems such as Firewall or Proxy.
  2. Before the Company's computers are connected to the network, antivirus software shall be installed and vulnerabilities in the operating system shall be patched.
  3. After using the Internet, users shall close the browser to prevent access by other persons.
  4. Users shall access information sources in accordance with the rights granted to them based on their duties and responsibilities in order to ensure the efficiency of the network system and the Company's security.
  5. Users shall not disclose the Company's important confidential information, except in accordance with the Company's official disclosure criteria.
  6. Users shall exercise caution when downloading programs from the Internet. This also applies to downloads for program updates. Such downloads must not infringe copyright or intellectual property rights.
  7. Users shall verify the accuracy and reliability of computer data obtained from the Internet before using such data.
  8. Users shall not use the Company's Internet network for personal business purposes or access inappropriate websites, such as websites that are contrary to public morals, websites with content that poses a threat to national security, religion or the monarchy, websites that pose a threat to society, or pornographic or obscene websites.

9. Users shall use the Internet in a manner that does not infringe the rights of other persons and does not cause damage to the Company. Users shall not commit any act constituting an offence under the law on computer-related offences or other relevant laws. In all cases where the Internet is used for the Company's operations, users shall strictly comply with the procedures prescribed by the Company.
10. Control of Access Rights Assignment for Users (User Access Control)
    1) Access to data and data processing equipment shall be controlled with due regard to the use and security of information systems. Criteria for granting access shall be established, and access rights shall be assigned so that users at all levels acknowledge, understand and can strictly comply with the prescribed guidelines and are aware of the importance of maintaining information system security and the confidentiality of important documents.
    2) Access rights to data and information systems, such as rights to use Application Systems and Internet access rights, shall be assigned to users as appropriate to their duties and responsibilities. Only the rights necessary for the performance of duties shall be granted, with written approval from an authorised person. Such rights shall be regularly reviewed in accordance with the procedures prescribed by the Company.
    3) Where it is necessary to use a User with special privileges, such use shall be strictly controlled. Refer to the section on the management of user rights with special privileges (High Privilege User).
11. Control of User Accounts (User Account) and Passwords (Password)

1) A system shall be established to verify the identity and access rights of users (Identification and Authentication) before access to sufficiently secure information systems is permitted, such as by setting passwords that are difficult to guess. Each user shall have an individual User Account. In determining whether password requirements and password controls are sufficiently robust, the Company shall consider the following factors as part of the overall assessment:

- Passwords shall be of an appropriate length. International standards generally recommend a minimum length of 8 characters (Alphabet + Numeric).
- Special characters should be used, such as ; : < > $ @ #.
- General users and users with special privileges, such as System Administrators and users associated with the system (Default User), shall change their passwords every 90 days.
- Passwords shall not be simple patterns or easy to guess, such as "abcdef", "aaaaaa", "123456", "password" or "P@ssw0rd".
- Passwords shall not be based on information related to the user, such as first name, surname, date of birth or address.
- Passwords shall not be words found in a dictionary.
- The number of unsuccessful password attempts (Logon Attempt - Retries) shall be limited. In practice, this should generally be set at 4 attempts. If the number of unsuccessful attempts exceeds the specified limit, the system or program shall not permit access or shall suspend access.
- Passwords shall be delivered to users in a secure and appropriate manner, such as in a sealed envelope.

• Users who receive a password for the first time (Default Password) or receive a new password shall change the password immediately.

• Users shall keep their passwords confidential and shall not write them on paper and attach them to the front of their computers. If a password is found to have been disclosed to another person, the user shall change the password immediately.

• For systems that use concurrent licences or Shared Users Licenses, such as the SAP system, the System Administrator shall send an email notification to the person responsible for such use to change the password for access to that system whenever there is a change in the users under that person's supervision.

2) Password files shall be encrypted (Encryption) to prevent unauthorised access or modification.

3) The list of users of important systems shall be regularly reviewed against the access rights table. Accounts of users who no longer have the right to access the system shall be reviewed, such as accounts of personnel who have resigned and accounts associated with the system (Default User). Access shall be suspended immediately when such accounts are detected, such as by disabling the account, removing it from the system, or changing the password. Clear guidelines shall also be established for granting additional access rights or modifying system access rights.

12. Management of Users with Special Privileges (High Privilege User)

Where it is necessary to use a User with special privileges, such use shall be strictly controlled. In determining whether the controls over Users with special privileges are sufficiently robust, the Company shall consider the following factors as part of the overall assessment:

• Approval should be obtained from an authorised person.

• The use of Users with special privileges should be strictly controlled, such as by limiting such use only to cases where it is necessary.

• The period of use should be specified, and access should be suspended immediately upon expiry of that period.

• Passwords should be changed regularly. In the case of intermittent use of High Privilege access, the Password shall be changed every time such use is completed. For users with special privileges, such as System Administrators and users associated with the system (Default User), passwords should be changed every 90 days or in accordance with the User Account and Password controls prescribed by the Company.

13. Remote Access Management

1) Users who need to access the system from outside, such as employees or Vendors, shall provide evidence stating the reason or necessity for such access to the IT Department in order to request the right to access the system remotely, and shall obtain approval from the executive of the IT Department or an authorised person before proceeding. Every user who accesses the Company's system from outside shall undergo identity verification. Identification shall be performed using the user's Username, and Authentication shall be performed using a Password, as prescribed. Remote access shall be subject to verification to authenticate the user, by means of a Password or an encryption method such as VPN/SSL.

2) The System Administrator shall be responsible for the security of remote access. Users shall strictly comply with the requirements for access to systems and data. Where necessary, the System Administrator shall require users to record their activities during remote system access as evidence for subsequent review.
3) Remote access shall be granted only as necessary. The System Administrator shall grant access only to the extent necessary and shall immediately close the access channel once the user has completed the required use.

6. Cryptographic Control

Objective

To prevent unauthorised persons from accessing, spying on, or modifying data or the operation of information systems in areas for which they do not have the relevant authority.

Guidelines

Data Management

1. Data shall be classified by confidentiality level. Data shall be categorised according to its purpose, and its level of importance shall be classified. Methods for managing each category of data shall be established, as well as procedures for confidential or important data before such data is cancelled or reused.
2. Important data transmitted through public networks shall be encrypted (Encryption) in accordance with international standards, such as SSL (Secure Socket Layer) or VPN (Virtual Private Network).
3. Measures shall be established to control the accuracy of data that is stored (Storage), entered (Input), processed (Operate) and displayed (Output). Where the same data is stored in multiple locations (Distributed Database), or where related datasets are stored, controls shall be established to ensure that the data is accurate, complete and consistent.
4. Measures should be established to maintain data security when computers are taken outside the Company's premises, such as when they are sent for repair, or data stored on storage media should be destroyed beforehand.
5. Where a user is not at the computer during working hours, measures shall be established to prevent use by other persons who do not have the relevant rights and duties, such as requiring the user to log out (Log Out) during periods when the user is not working at the computer.

1. Where it is necessary for a user who owns important data to grant another user the right to access or modify the data owned by that user, such as Share Files, such rights shall be granted only to specific persons or groups. Such rights shall be revoked when they are no longer necessary. The data owner shall retain evidence of the granting of such rights, specify the period of use, and suspend such rights immediately upon expiry of that period.

2. Where it is necessary to grant rights to another person to access information systems and network systems on an emergency or temporary basis, procedures or methods shall be established, and approval shall be obtained from an authorised person on every occasion. The reason and necessity shall be recorded, the period of use shall be specified, and such rights shall be suspended immediately upon expiry of that period.

7. Security of Information Technology Operations
(Operations Security)
Objective

To ensure that the Company's information technology system operations are carried out correctly, securely and safely, to prevent data loss, and to protect the systems from malicious programs.

Guidelines

1. Manuals or operating procedures shall be prepared for the Company's important information technology systems to prevent errors in information technology operations.
2. Information shall be backed up before any changes are made to the information.
3. A system should be installed to monitor the resources of information technology systems, such as CPU, Memory and Hard Disk, to determine whether they are sufficient. The monitoring data shall be used to plan increases or reductions in resources in the future.
4. Systems of high importance should have the development system separated from the actual service system in order to maintain system security and prevent errors or unauthorised changes to data.
5. Data shall be surveyed in order to classify its level of importance, identify the data to be backed up, and determine the frequency of data backups.
6. Important data shall be backed up frequently, and arrangements shall be made to transfer backup data for storage outside the Company's premises.
7. The readiness of the information technology system backup system shall be tested at least once a year.
8. Measures shall be established to prevent programs that may cause damage to information technology systems. For example, personal computers or portable personal computers from outside the Company shall be connected to the Company's network through VPN.
9. Antivirus software shall be installed, and vulnerabilities in operating systems and web browsers shall be patched.
10. Users shall regularly update the operating systems and programs they use with released Patches and/or Hotfixes. These may be downloaded from the product owner's website to address vulnerabilities.
11. Users who wish to install software other than that prepared by the Company shall notify the Information Technology Department so that its security can be checked. The Information Technology Department shall be the only party responsible for installing such software.

8. Security of Information Communications through Computer Networks
(Communications Security)
Objective

To protect information in the network from access by persons, viruses and various types of malware that may access or cause damage to data or the operation of information technology systems.

Guidelines

1. Management of Network Security (Network Security Management)
    1. Controls shall be established to ensure secure access to the network.
    2. The network shall be separated between internal users and external users who connect to the Company.
2. Information Transfer (Agreements on Information Transfer)
    1. Agreements on Information Transfer shall be established with due consideration to information security. The System Administrator shall control such operations to ensure security in all three areas: confidentiality (Confidentiality), accuracy of information (Integrity), and readiness to provide services (Availability).
    2. An agreement shall be signed between the Company and external organisations under which the external organisations agree not to disclose the Group's confidential information (Non-Disclosure Agreement: NDA).

9. Management of Incidents That May Affect Information System Security
(Information Security Incident Management)
Objective

To establish appropriate and effective methods for managing information system security incidents, as well as for reporting the status of information system security and information system security vulnerabilities.

Guidelines

1. Responsibilities and operating procedures shall be established to deal with incidents related to the Company's security.
2. Clear communication channels shall be established for reporting information system security incidents.
3. If users identify an incident that may affect information system security, they shall report the incident to the Information Technology Department.
4. Information Technology Department personnel shall assess the severity of the incident. If the incident has a severe impact on a large number of users, an urgent announcement shall be made.

10. Information System Acquisition, Development and Maintenance
(System Acquisition, Development and Maintenance)

Objective

To control the development or modification of information systems so that computer systems that are developed or modified process data accurately and completely and meet users' requirements.

Guidelines

1. Written procedures or operating methods should be established for the development or modification of systems. At a minimum, requirements should be established for the request process, the development or modification process, the testing process, and the system transfer process.
2. Procedures or operating methods should be established for emergency changes to computer systems (Emergency Change). The reason and necessity for each change shall be recorded, and approval shall be obtained from an authorised person on every occasion.
3. Details of such procedures shall be communicated thoroughly to users and relevant persons, and compliance with the procedures shall be controlled.

Control of System Development or Modification

1. Request
   - Requests for the development or modification of computer systems shall be made in writing in accordance with the prescribed procedures and shall be approved by an authorised person, such as the head of the requesting unit or the person responsible for the information system.
   - The impact of significant changes should be assessed in writing in terms of the operation (Operation), security system (Security), and functionality (Functionality) of the relevant system.
   - Relevant regulatory requirements should be reviewed, as changes in many cases may affect compliance with such regulatory requirements.
2. System Development Procedures
   - Computers used for system development (Develop Environment) shall be separated from those used for actual operations (Production Environment), and access to each environment shall be restricted to relevant persons only. Such environments may be separated by using different computers or by separating the environments within the same computer.
   - The requester and relevant users should participate in the development or modification process to ensure that the system is developed in accordance with their requirements.
   - The security (Security) and availability (Availability) of the system should be considered from the initial stage of development or modification.
3. Testing
   - The requester, the Information Technology Department and other relevant users shall participate in testing to ensure that the computer system that has been developed or modified operates efficiently, processes data accurately and completely, and meets requirements before it is transferred for actual use.
4. Transfer of the System for Actual Use
   - The transfer of the system for actual use shall always be checked for accuracy and completeness.

5. Preparation of Documents and System Development Details, and Retention of Versions of the Developed System
   - Details of the programs currently in use shall be retained, with details of previous development or modifications.
   - All system documentation shall be updated after development or modification to ensure that it is always up to date, such as data structure documentation, system manuals, user registers, program operating procedures and Program Specifications. Such documents shall be stored securely and in a manner that facilitates their use.
   - The previous Version of the program before development shall be retained for use in the event that the current Version malfunctions or cannot be used.
6. Post-Use Testing (Post-Implementation Test)
   - The developed or modified system should be tested after it has been in use for a period of time to ensure that it operates efficiently, processes data accurately and completely, and meets users' requirements.
7. Communication of Changes
   - Changes shall be communicated thoroughly to relevant users to ensure that they can use the system correctly.

11. Use of Information System Services from Service Providers (IT Outsourcing)

Objective

To protect the assets of the Group that are accessed by IT Outsourcing and to maintain the agreed level of security and level of service as specified in the service agreement.

Guidelines

1. Security requirements for the Group's information shall be established where IT Outsourcing needs to access the Group's information or information assets, in accordance with the requirements relating to the confidentiality of the Group's information.
2. Security requirements for the Group's information shall be communicated and enforced where IT Outsourcing needs to access the Group's information or assets before such access is permitted.
3. The service agreement shall require regular monitoring, review and assessment of services provided by external service providers.
4. If there is any change to a service agreement for an important system, an information security risk assessment shall be conducted.

12. Business Continuity Management in Relation to Information System Security (Information Security Aspects of Business Continuity Management)

Objective

To prevent disruption to the Company's operations arising from a crisis or disaster and to prepare the Company's information system equipment for operational readiness.

Guidelines

1. The Information Technology Department shall prepare a plan to address uncertain situations and disasters that may affect information systems, in accordance with the Company's Crisis Management Plan.
2. Information system risks that may arise shall be reviewed and assessed at least once a year.
3. The emergency preparedness plan shall be reviewed at least once a year.
4. The readiness of the backup information system shall be checked at least once a year.

13. Personal Data Control (PDPA)

Objective

1. To ensure that executives, Officers and external persons who work for the Company recognise the importance of the privacy of Customers, Officers and external persons who work for the Company.
2. To establish standards and guidelines for executives, Officers and external persons who work for the Company to perform their duties in compliance with the personal data protection law.
3. To ensure that executives and Officers at all levels are informed of and strictly comply with this Policy.

Guidelines

1. Personal Data related to the Company's business operations shall be regarded as an asset of the Company. Executives, Officers and external persons who work for the Company have a duty to protect and keep such Personal Data confidential and shall exercise caution when using such Personal Data, regardless of its form.
2. Executives and Officers of the Company shall collect Personal Data only to the extent necessary for the Company's operations. Where Personal Data received is unnecessary or unrelated to the performance of duties, executives and Officers of the Company shall make such Personal Data incapable of identifying the individual or make it impossible to view such data.
3. Executives, Officers and external persons who work for the Company have a duty to prevent and exercise caution to avoid Security Incidents or Undesirable or Unexpected Security Situations.
4. Executives, Officers and external persons who work for the Company have a duty to take care of and be responsible for the Company's assets entrusted to them for the performance of their duties as if such assets were their own.
5. Executives, Officers and external persons who work for the Company shall not copy, reproduce, disclose, disseminate, modify, alter, duplicate, distribute, transfer or destroy such data without permission from their supervisor or a person authorised by their supervisor. If the Company determines that such data has been copied, reproduced, disclosed, disseminated, modified, altered, duplicated, distributed, transferred or destroyed without permission from the supervisor or a person authorised by the supervisor, the relevant executive, Officer or external person shall be responsible to the Company for any damage arising or that may arise from such incident.

6. Where it is necessary to disclose Personal Data to a person or juristic person who is not an executive or Officer of the Company, the Company's executives and Officers shall comply with the Company's policies and guidelines on information security and any other methods prescribed by the Company to prevent such person or juristic person from storing, collecting, using or disclosing Personal Data without authority or without due justification.
7. Personal Data, sensitive Personal Data and other information related to the Company's business operations that executives, Officers and external persons who work for the Company have obtained shall be used solely for the Company's operations. Such information shall not be disclosed or used for any other purpose not prescribed or authorised by the Company, nor shall it be disclosed or used in a manner that may cause damage to the Company.
8. Applicable laws and laws to be promulgated in the future, as well as the Company's policies, rules, regulations and requirements, are important matters to which executives, Officers and external persons who work for the Company shall give due importance and strictly comply. They shall not commit or participate in any violation of such laws, policies, rules, regulations or requirements.

This Policy shall be effective from 20 December 2023.

(Mr. Pumipat Sinacharoen)
Chief Executive Officer

Proposed by _____ (Mr. Kornwara Sai-intr) VP of Business Process Improvement and Information Technology

Information Technology Department
Note: Directors, executives and employees shall be notified through the email system.