-**Translation**-

Information Security Policy

Effective on 15 August 2018

This policy is established as guidelines so that the users and the relevant persons are aware of importance of information security and know the duties and practices for controlling or reducing the likelihood of various risks. The content covers policy guidelines, policy details and compliance

so as to control the operation and information security of the Company effectively in the same standard level.

Section 1: Meanings and definitions

The objective is to provide the definitions related to the policy so that the relevant persons know and understand the content consistently.

1.1 Computer Asset means all assets related to the use of computer system such as hardware, software and information, etc.

1.2 Server means the computer in the network that serves as the center of operation such as storage of data or software for service to other computers or controlling the operation in the network.

1.3. Remote to Network means connection of the computer or network to other computers or networks via other communication devices or signal mediums, e.g. Modem, VPN IP Router.

1.4 Access Control means the control of access or use of computer asset in accordance with the specified rights only.

1.5 Computer means equipment used to process information electronically by executing the commands through software to get the desired results such as Server, computer, Personal / PC / Desktop Computer and Notebook / Laptop Computer.

1.6 Computer Accessories mean electronic equipment for use together with the computer

so that the computer can operate as required and include the computer.

1.7 Signal / Network link / Lan mean any medium used for connection between computer accessories, e.g. copper wire, fiber optic, Wifi network.

1.8 Hardware means computer accessories or the computer's components

1.9. Software / Application Software means a set of commands for the computer to operate

as desired, such as Microsoft Office, Adobe Acrobat

1.10 Specialized Programs means the developed program using for the special objectives such as Accounting Program (Winspeed), Weight Scaling Program

1.11 Application means the supporting program for the operation which free download. Other applications shall be approved by the IT such as Line PC program

1.12 Information technology system means the work system of the department using information technology, computer system and network system to help create information, which can be utilized by the department for planning, management, service support, development and control of communication, which includes the components, e.g. computer accessories, network system, program, work system and information.

1.13 Information refers to processed data, organizing information in the forms of numbers, text or graphics in a way that the users can easily understand and use for management, planning,

decision-making and more.

1.14 Work system refers to the application of information technology to operation in order to achieve the set objectives such as accounting system, salary and wage calculation system, weighing system through the scale, etc.

1.15 Operating System (OS) refers to software controlling the operation of computer and allocating system resources, including memory management, control of data input devices (keyboard, mouse) and display equipment (screen, printer).

1.16 Firewall means a security system consisting of computer accessories and software. The functions are to prevent unauthorized persons of external network from using the system and restrict the use of internal users in accordance with the policy specified by the Company.

1.17 Information / Data means the text, command, a set of commands or anything else in the computer system in a state where the computer system can generate, send, receive, store or process electronically on computer accessories. It also includes electronic data according to the law on electronic transactions.

1.18 File means the data collected into record medium and identified as a unit with specific name such as software applications and document files created and named, then saved in record medium, etc.

1.19 User means the officer or outsider entitled to use information technology system of the Company.

1.20 Network Administrator means the person responsible for managing and maintaining the network.

1.21 Host / Server Administrator means the person responsible for managing and maintaining the host computer.

1.22 Firewall Administrator means the person responsible for Firewall management and maintenance.

1.23 User Account means the user's account for accessing and using information technology system in accordance with the agreement between the user and the information service provider.

1.24 Administrator Account refers to the account used by the host computer administrator for host computer administration.

1.25 Configuration document means the document that details various configurations in the information technology system so that this system can use as required.

1.26 Risk refers to the likelihood of computer asset for violated information technology security.

1.27 Staff means the employees of the Company.

1.28 Virus means the attempted installing software without permission or operated by the maleficence which will affect to the computer or IT information system or to destroy, modify, change other commands that not accord to the specified desires.

1.29 Spam, Malware means the malicious developed programs by the programmer for the various objectives such as hacker or information input recording to take the secret information in the computer such as username, password and private information for log-in which typed by the user. In general, the hacker will install the malicious program into the computer to steal the information and hack the system or attack to the server and network that are well known as the Denied of Services Program.

1.30 Outsource means the organization permitted by the Company to access or use the Company's information or information technology system by getting access according to use type and taking responsibility for not disclosing the Company's secrets without authorization.

Section 2: Security Policy

The objectives are to direct and support the implementation of security for the Company in accordance with or in compliance with applicable legal and regulatory requirements according to audit standards from outsource in the field of IT General Audit.

2.1 When this policy becomes effective, the department responsible for information technology must issue the rules, requirements and regulations necessary for information system and computer network security of the Company by approval of senior management. Besides, the administration department provides support for the policy, budget, resources and more necessary for continuous improvement of information technology and computer network security.

2.2. Dissemination of the policy on information technology and computer network security to staff, outsource service providers and the relevant people to get informed and put into practice.

2.3. Review and evaluation of the policy on information technology and computer network security at least once a year or in case of important changes affecting information technology and computer network security of the Company.

Section 3: Organization of Information Security

3.1 Structure of information security within the organization (Internal Organization)

The purposes are to manage and designate the department responsible for security of information technology and computer network of the Company.

3.1.1. Senior management assigns the representatives or working group from various departments in the Company to coordinate or collaborate in creating security for information technology and computer network of the Company. Such representatives or working group must have

clearly defined responsibility for information technology and computer network security of the organization.

3.1.2 The representatives or working group appointed by senior management are responsible for managing and controlling security of information technology and computer network of the organization and reviewing the policy on information security management by creating the procedures and guidelines for maintaining security of information technology and computer network and documents related to security of information technology and computer network.

3.1.3 Company staff must not disclose the Company's secrets, unless authorized to disclose by the Company.

3.1.4 Required audit of the operation and practices related to information technology and computer network by independent auditor at the prescribed time or in case of changes crucial to the Company.

3.2 Security structure related to customers or outsource agencies (External Parties)

The purpose is to manage security for information and data processing equipment of the Company, which are accessed, processed or used to communicate with the customers or outsource agencies.

3.2.1 Required assessment of the risk of access to information or data processing equipment by outsource agencies and specified measures to support or modify appropriately before allowing access.

3.2.2 Required identification and enforcement of security requirements for

the Company's information when it is necessary to allow the external parties or the visitors, outsource audit agency to access information or information asset of the Company. Before allowing access,

there is need to identify and establish the requirements or agreements related to information security between the Company and outsource agencies when it is necessary to allow such agencies to access the Company's information or data processing equipment before allowing access.

Section 4: Asset Management

4.1 Responsibility for Assets

The purpose is to manage security for information and data processing equipment of the Company, which are accessed, processed or used to communicate with the customers or outsource agencies.

4.1.1 Required preparation and revision of the list of assets important to the Company correctly and regularly, including identifying ownership of the assets.

4.1.2. Written rules or criteria must be established for the use of information and assets related to information processing properly to prevent damage to such assets such as lack of caution, lack of care and attention.

4.1.3 It is necessary to keep the assets important to the Company neatly and tidily in a safe and appropriate place.

4.1.4 Permission to use Computer equipment is as follows.

- All information technology systems and related data processing equipment provided by the Company are intended for working according to the Company's missions.
- The use of systems and devices for personal business is allowed to the extent as appropriate, which must not hinder or interfere with the duties of staff.
- Staff as well as the persons and / or juristic person employed by the
- Company must be responsible for computer equipment provided for use and monitoring these resources for security and accuracy, including information and information systems of the Company.
- The users must be responsible for carefully handling computers

and devices of the Company and providing protection like their property.

- All Client computers, portable computers (Laptop/Notebook) and Server of

the Company must be protected by passwords of operating system every time of access and must be protected automatically by password of Screen Saver or Log Off every time when not using equipment for a period of time.

- For working off the premises, the users must take care of and be

responsible for computer equipment of the Company assigned.

- The users must not connect their personal computer to the Company's network and must not install any software on the Company's computers before getting permission of the information technology department.
- Portable computers (Laptop / Notebook) provided by the Company for use with stored confidential information must be protected like computers in use within the Company, e.g. the need to install anti-virus software, anti-spyware software and always update Security Patch, etc.
- Computer equipment of the Company must be neither modified nor equipped with any additional device before getting permission from the administrator of that department. Besides, staff must not allow any irrelevant person to install any hardware or software on the Company's computers strictly.

4.1.5 Permission to use Software is as follows.

- Staff is not allowed to install or distribute pirated software on the Company's computer system.
- Software to process and store confidential or important information of the Company, which has been developed by users or purchased, must be checked, controlled and appropriately approved by the department owning system or data before installation on information technology systems of the Company.
- All information systems used by general users must have sufficient supporting documents to enable the Company's general users to understand and use information systems.
- The list of software or information systems installed on the users' computers must be documented and approved by the senior management to ensure that such software is properly copyrighted and installed for work purposes of the Company only.

4.1.6 Permission to use the Internet is as follows.

- The Company provides Internet service to support the operations and help staff in searching for information, knowledge and communication with third parties to enhance the Company's performance and services.
- The users must use the Internet with caution. This use must not defame the reputation of the Company and people relevant to the Company or related to the offense.
- The misuse of the Internet is disciplinary offense and may be prosecuted by law.
- Access to the Internet requires access through authorized Gateway or via client computers provided for use only.
- Do not use popup window or log in to any website advertised by Spam because these websites may have malicious programs hidden or may steal information on the users' computers without the uses' awareness or permission.
- The users are not allowed to visit, download or reproduce pornographic media and any other media that are inappropriate or illegal.
- The Company does not support the expression of personal opinions in electronic form (e.g. via web board or blog) of staff. Any potential damage from such comments is the responsibility of that staff.

4.1.7 Permission to use Email is as follows.

- All users of the Company must have their own E-mail Account.
- To create the new user or delete the user's account shall submit the document (Doc no. IT2019-001) to IT staff for email applying or canceling
- E-mail Account must be protected by password to prevent encroachment and the misuse of email.
- All Email Accounts and emails (including personal emails) created and stored on the computer system or the network of the Company are the Company's assets.
- The users must use only authorized software to access and / or communicate with the Company's email system.
- The Mail Box Size of the users is limited. When the volume of emails exceeds storage space, the users will not be able to send - receive emails as usual. The users should delete the unimportant emails and free the Mail Box's space
- The size of email attachments is limited. If email attachments are larger than the specified size, the users will receive a bounce message stating that such email cannot be sent.
- The users must always delete unnecessary emails from their Mailbox to maintain email storage space according to the Company's specified size. The users must keep emails connected with working and emails as required by law only.
- Do not use the Company's E-mail Account to do anything related to illegal things such as advertising intoxicants, contraband, distributing pirated software.
- Do not use the Company's E-mail Account to post any information in the electronic community such as web board, blog, bulletin board, unless such posting is relevant or part of working for the Company.
- The e-mail software must be set for every sent email to have the sender's signature always. That signature must include the name- surname, position, department name, company name and telephone number.
- The document file attached to email must be in standard format, which can be read by recipient with basic software on all operating systems such as PDF, DOC, TXT, XLS, JPG, GIF, PPT, etc.
- The users are prohibited from copying the text or confidential attachments from other people's emails without permission of the owners.

- The users must carefully draft the content of emails by always bearing in mind that they are the senders of such emails on behalf of the Company.
- The users must not allow others to send emails using their E-Mail Account strictly, whether those persons will be the supervisor, secretary, assistant or any other person.
- The users are not allowed to send emails, which are not wanted by the recipients, e.g. Junk mail or Spam mail.
- The users are strictly prohibited from creating or involving in sending any fraudulent email or chain email.
- The users are not allowed to send or forward any e-mail with the content or images that are defamatory, slanderous, racist, threatening, obscene, sexually provocative or email with the content at risk of cultural or religious issues and emails that affect national security or the monarchy strictly.
- The users are not allowed to send emails with attachments related to gambling, pornography or any other file that is not related to working and adversely affect the Company.
- The users must exercise special caution when opening attachments received from unknown senders. These attached files may contain viruses, email bomb or hidden program (Trojan Horse).
- When receiving a message from anti-virus software warning that their computer has the virus, the users must immediately stop sending emails until the computers will be repaired and return to normal.

4.1.8 Permission to use telephone, fax, printer and copier is as follows.

- If the users receive information from erroneously faxing such as faxing to the wrong number, division, etc., the users must notify that fax sender and destroy such document.
- The users are not allowed to print confidential information with the printer located in the common area, unless authorized person waits for the document coming out of that printer.
- Do not talk about confidential information through Speakerphones or through any electronic media such as telephone turning on the speaker phone during the teleconference, unless the attendees of all departments have been identified as relevant persons and being entitled to get informed.
- The relevant persons have already checked and ensured that no unauthorized person in the vicinity may hear confidential information of the conversation.
- The teleconference is held in secure areas, e.g. a meeting room with proper walls and doors that can prevent the sound coming out.
- The users must obtain permission from information owner before copying or scanning the document containing confidential information.

4.2 Information Classification

The purpose is to handle the Company's information so as to be protected in appropriate level.

4.2.1 The documents must be classified and prioritized (Classification Guidelines) for secure information management by the proper methods.

4.2.2 The documents or publications printed or reproduced from the originals classified, e.g. confidential documentation are considered as original confidential documents that are digital or digital information.

4.2.3. The method of making and handling name tags for information documents and Asset information Tag related to information technology management must be available.

4.2.4. Information in the form of document must be properly controlled and secured from printing, making name tags, storage, reproduction, distribution and destruction. The rules must be

established for staff to follow to ensure that controlled and secured information, confidential information must not be disclosed to others, except the necessity for working only.

4.2.5. The users must be aware of protecting data stored on the users' computers, especially the computers shared with more than one person. This confidential information must be protected by coding or any other means of operating system or information systems appropriately.

4.2.6 Confidential information must be kept out of processing devices such as printer, fax machine, copier immediately.

4.2.7 Staff must not disclose confidential information to outsiders, except that disclosure is covered by the disclosure agreement.

4.2.8 Staff must neither discuss nor use the Company's confidential information in public areas such as elevator, restaurant.

4.2.9 Data media and portable computer accessories such as Thump-Drive, CD -Rom, External Hard disk drive containing the Company's recorded confidential information must be carefully maintained and used.

4.2.10 All important information related to the Company's operations, which is stored on the users' computers or host computer managed by users, must be backed up regularly for data recovery in case of any problem, e.g. virus infection, broken hard disc.

Section 5: Human Resources Security

5.1 Building security for staff involved in information operation, including educating the employees to be able to protect against various risks.

The purposes are to manage staff to be aware of the risks associated with information operation and educate the employees to be able to protect against such risks.

5.1.1 Staff or the users are responsible for studying, understanding security practices of information systems specified by the Company to implement security for computer assets in their use or responsibility.

5.1.2 Disciplinary punishment must be imposed on those who violate

the Company's policies, rules and / or regulations. However, for violation of laws, penalties will be based on the offense as stipulated in each of the legal provisions.

5.2 Canceling access of staff with terminated employment

The purpose is to manage cancellation of access of staff with terminated employment or contract expiry for information system security.

5.2.1. So that management of Login or User ID is the most accurate and up-to-date,

the human resources department must notify the information technology department immediately when the following cases occur.

- Employment
- Changes in employment conditions
- Resignation or termination of being the executive, staff and employee or death
- Transfer of department
- Suspension from job, disciplinary punishment or suspension from duty

Staff and the employees with terminated employment must return all assets related to computer system, including the key, staff identity card (if any), entry and exit card (if any), computers and peripherals, manuals and documents to the supervisors before the last day of employment.

After cancellation or change of position as staff and employee, it is necessary to notify cancellation of access to information of the department and inform staff and other employees, customers, partner companies, Third Party / Outsource involved as appropriate.

If the above changes affect to the users changing or access grants in the Company's programs, it is required the submission of the document (Doc no. IT2019-001) to inform the IT staff for the said changes and proceed for the access grants or cancel the related user ID.

Section 6: Environment and Equipment Security

6.1 Computer equipment and information storage facility must have a secure and appropriate environment.

The purpose is to handle the storage facility to be secure and appropriate.

6.1.1. The facility or space for storing computer equipment or related accessories, including important information must be in a secure and suitable location, including the availability of person responsible for the environment for security. The signs should also be available, which indicate the places that do not allow third parties to access the areas of important equipment storage. Also, the tags must be available to indicate staff responsible for equipment storage facility at all points clearly.

6.1.2 Information, recording media, materials and equipment stored must not be left alone on the desks in the meeting room or in the cabinet that are not locked with key.

6.1.3 Staff must not allow any person to move computers or the recording media from their work area, unless that person is staff authorized to act and action is correctly taken according to the policy, order of the department responsible for the Company's information systems.

6.1.4 For security of the facility for installed and stored computers, it is necessary to provide protection against risks such as fire, natural disasters or theft or other potential occurrences.

6.2 Equipment Security

The purposes are to manage the prevention of unauthorized use of computer equipment and to ensure that computer equipment is adequately protected from potential risks.

6.2.1 Staff or the users must put and protect the Company's equipment to minimize the risks of environmental and other hazards, including unauthorized access to equipment.

6.2.2 Preparations must be made for protective equipment, which must be maintained in order to prepare protective equipment to be readily available such as UPS. Staff and the users are responsible for monitoring to test protective equipment to be ready for protection.

In case of power failure, protective equipment must be ready to use always. If protective equipment is defective, the relevant department must be notified, which is responsible for system to provide backup equipment to replace or provide replacement equipment if finding faulty protective equipment.

6.2.3 Various devices must be regularly maintained. Staff and the users as well as the responsible persons in charge of areas must regularly maintain various devices to keep equipment working continuously in perfect condition to use.

6.2.4 Staff or the users must liaise with the information technology department to prepare a support plan in case of damaged computer equipment and test a support plan by the reasonable period of time.

6.2.5 Staff or the users must check equipment containing the recording media to determine whether important information and copyrighted software in such recording media have been removed or overwritten before donation, getting rid of or sending that equipment to the external agency for repair so as to protect such information.

6.2.6 Assigning staff of each department to maintain computer equipment and control the transfer of computer equipment to prevent data stored on computer equipment from leaking or modification.

Section 7: Communication and Operation Management

7.1 Determination of responsibilities and operational methods

The purposes are to operate and manage information infrastructure correctly and safely.

7.1.1 The information technology department must prepare the information manual and / or operational procedures in the department such as procedures for notifying failures, recovery, system maintenance. This includes detailed procedures for practice, explaining, distributing or assigning staff or the department in the storage area to take responsibility for implementing the procedures specified.

7.1.2 The information technology department must change the network, computer system, equipment, software. Every change must be communicated and recorded. The relevant department must be informed about change details. The information technology department must determine responsibility for operation related to information systems and network clearly so as to avoid the misuse of assets or the use without permission.

7.2 The case of outsourcing requires the management of external service provider.

The purpose is to provide and maintain the level of information security and the level of service appropriate and consistent with the service agreement with the outsource agency (if any).

7.2.1 The agreement must be made to regulate information technology service of the outsource agency by including the following details.

- Acceptance of the Company's information security policy and control
- Scope, details and level of service (Service Level Agreement)
- Documents on measures for controlling Confidentiality, Integrity and Availability
- Network link agreement of the outsource agency
- Information that the outsource agency can have access and the procedure as well as method for requesting information of the Company if needing more information
- Non-disclosure agreement of the Company
- Legal requirements such as Privacy and data protection
- The information technology department must review management of change in service of the outsource service provider (if using Outsource service).

7.3 Control and Protection against malicious

The purpose is to control and protect the users of software system, data and equipment against malicious purposes or unwanted activity.

7.3.1 Computers, portable computers to use through the Company's network must be registered and authorized according to security policy before approval for use in the system.

For registration of equipment, the registration information must be sent to the IT department of the Company.

7.3.2 Client computers and portable computers (Laptop / Notebook) must be equipped with the latest antivirus software approved by the IT department and must be activated all the time of using the machine.

7.3.3 Staff is not allowed to download shareware or freeware directly from the internet without approval of the IT department. After approval, staff must scan software with the virus detection program before use.

7.3.4 All files downloaded in the department are email attachments, copies from disc or shared files, which must be scanned for viruses.

7.3.5 The users are not allowed to create, store or distribute any malicious programs such as viruses, Internet worm, hidden program (Trojan Horse), email bomb into the Company's computer system.

7.3.6 The users are not allowed to hinder or interfere with the function of antivirus software. Only work-related files are allowed to receive, send through the Company's network.

The users should receive files from known persons and from the possible communication channels only. In addition, the users must always scan the virus on files received by the Company's antivirus software before activation.

7.4 Network Security Management

The purpose is to protect data in the network and protect infrastructure supporting the Company's network.

7.4.1 The users are not allowed to install any hardware or software related to network services, e.g. Modem, Router, Switch Hub and Wireless Access Point without permission strictly.

7.4.2 For connection to external network for Outsource or service provider to solve the problems, fix system problems, the users are prohibited from connection to external network without permission from the head of that department or the users do not monitor the screen to see work processes or control the wrong operation.

7.4.3 The information technology department should limit the number of external connections to the Company's network and require connections to specific computers and specific work systems only. Besides, such computers and work systems should be separated from

the Company's actual network in physical and Logical terms. Moreover, the external agency must not be allowed to access the Company's computers or network system.

7.4.4 All corporate networks connected to other networks should be equipped with

basic software for virus detection and prevention. Or it is advisable to provide Firewall equipment to protect against attacks from malicious users or unauthorized connection.

7.4.5 The information technology department should prepare responsibilities and

practices in case of malfunctions and guidelines for checking malfunctions in various cases, including the solution manual if finding the problems, faults or violations that affect the Company's network.

7.5 Management of the recording media for security (Media Handling)

The purpose is to prevent potential damage to the recording media.

Each department should establish the methods for authorizing system users to use the recording media (Thump drive) or (External Hard disk drive). Information on such media users should be registered to record information that is distributed or requested of people with access by Update regularly.

7.6 Exchange of Information

The purposes are to prevent the loss of information and software and to prevent unauthorized modifications or inappropriate use of information.

7.6.1. The information technology department must determine the methods for storing the recording media (information or software) for security.

7.6.2 The information technology department must determine the methods for preventing access to electronic information and electronic data transmission via the network.

7.6.3 The information technology department must proceed the virus scan of the extended sources such as flash drive, the external HDD by installing the virus protection program into the computer.

7.7 Security Monitoring

The purpose is to detect unauthorized information processing activities.

7.7.1 The information technology department must record the activity (Audit Logging) of the users, denial of service and the cases related to security regularly.

7.7.2 The information technology department must inspect the use of information assets regularly to check whether something went wrong or not.

7.7.3 The information technology department must require protection of information, recording the activities or cases related to the use of information for preventing unauthorized changes or modifications.

7.7.4 The information technology department must record the operation of staff connected with the system (Administrator and Operator Logs).

7.7.5 The information technology department must record Fault logging related to the use of information, analyze such faults and take corrective action as appropriate.

7.7.6 The information technology department must synchronize all computers in the department (Clock Synchronization) based on the correct time source to help in verifying the period if the Company's computers are compromised.

Section 8: Backup and Server recovery policy

8.1 Server Back-up Policy

The purpose is to guide the backup approach for system recovery in case of circumstances such as defective equipment, brownout or power surge causing damage to the system or natural disasters, accidents, etc.

8.1.1 The information technology department must back up data once a week regularly.

8.1.2 The information technology department must control access to the server room for data security.

8.1.3 The information technology department must have a backup process with 2 backup locations, including 1. place of available data 2. off the premises to prevent various risks that will occur.

8.1.4. The register of backup record must be available.

8.1.5 Storage of data media at the storage facility must be recorded and checked annually.

8.1.6 The process of data media storage and the backup storage facility must be checked at least once a year.

8.1.7 The media to store information must have detailed tags, which include at least the following information: system name, creation date, importance of data, contact details of data administrator.

8.2 Recovery Policy

8.2.1 The information technology department must test data recovery on a regular basis

every half year.

8.2.2 The information technology department must have an emergency plan for handling the risks.

8.2.3 The information technology department must have backup data both on and off the premises to prevent the risks.

Section 9: Access Control

9.1 Business Requirement for Access Control

The purpose is to control access to data and information systems for security.

9.1.1 The information technology department must develop the policy

and requirements for using data and information systems to control access of authorized persons only.

9.1.2 The information technology department must determine access to data and information systems to be appropriate for access and responsibilities of the users before accessing information technology systems. Also, access must be regularly reviewed. The users must be authorized by the system administrator as needed for use.

9.1.3 Only the administrator can modify access to data and information systems.

The information technology department must record and track the use of the Company's information technology systems and monitor breaches of important data and information system security.

9.2 User Access Management

The purpose is to prevent unauthorized users from accessing information systems.

9.2.1 New user registration. Formal rules are required for registering new users to have the rights to use as needed, including the regulations for cancelling access such as the cases of resignation or change of position within the Company, etc. The users must be reviewed and approved according to the Company's procedures strictly.

9.2.2 The users' access to each information system must be determined, including separate access according to responsibilities. The users' identity must be verified every time of Log-on to information systems.

9.2.3 The information technology department must handle the users' passwords for security always. The information technology department must review access to information systems by the specified period (e.g. at least 1 time in 6 months, etc.).

9.2.4 The record of access and use of each information system (LogFiles) must be stored for at least 5 years.

9.3. User Responsibilities

The purpose is to prevent unauthorized persons from access to information systems.

9.3.1 The administrator responsible for system must determine the users' access to each information system and access of each user.

9. 3. 2. Staff must comply with the Company's information access control, change and cancellation of passwords and password use management.

9.3.3 If special access must be given to the users, namely the users with maximum rights, it is necessary to control such privileged users tightly enough by using the following factors for consideration.

- Approval should be given by the supervisor and the system administrator.
- The use should be strictly controlled, e.g. control of the use in necessary cases only.
- The period of use should be fixed and the use should be stopped immediately after that period.
- The passwords should be changed strictly such as every time after the need to use or if it is necessary to use for a long time, the passwords should be changed every 6 months, etc.
- Shall strictly proceed the password change such as no longer necessary to use or necessary to use for the long term. The password should be changed in every 90 days.

9.3.4 The users must be responsible for maintaining their own User Name and Password as well as personal data that may be used to change account information for security regularly.

9.3.5 The passwords must be as secure as specified.

9.3.6 The passwords are confidential information. All users are responsible for maintaining their password securely. Do not share Account or let others use their Account strictly. This includes family members when the users bring work to do at home as well.

9.3.7 The users must be responsible for any action taken through their User ID and password. If the users suspect that their User ID or password have been compromised, the users must notify the information technology department and make all changes to the password immediately.

9.3.8. The project managers of new systems in the Company must ensure that the systems in their charge are consistent with the content of this policy and all other supporting documentation and must liaise with the system administrators to control and adjust system settings to meet all relevant requirements before the actual use.

9.3.9 Reset Password must go through the Company's standard process only to ensure compatibility with User to Reset the password actually. Besides, the system administrator is entitled to request information and verify the user's identity as appropriate.

9.3.10 On the other hand, the user may be requested by the information technology department to change the password again if the user's password is not secure, can be guessed or easily compromised. The user must also verify the source of that request to ensure that such request is not trickery.

9.4 Network Access Control

The purpose is to control the use of services on the Company's network.

9.4.1 The information technology department must establish the approach / policy on controlling access to the network and network services specifically to prevent unauthorized access.

9.4.2. The Network Diagram must be created with detailed scope of internal and external networks and devices, which must be always updated.

9.4.3 The information technology department must restrict access so as to control the users to use authorized networks only. The information technology department must restrict access to shared networks.

9.5 Operating System Access Control

The purpose is to prevent unauthorized use of operating system.

9.5.1 The information technology department must provide the systems or procedures for checking the passwords' quality. Also, the method must be available to control system users to change the passwords by the specified time.

9.5.2 The information technology department must provide for the control of using the utility program for system to prevent unauthorized access as follows.

- The verification of identify is required before use.
- The utility program must be separated from the system program.
- The use of utility program must be limited to assigned persons only.
- The details of utility program access must be recorded such as system users.

9.5.3 The information and communication technology group must have a way to cut the time of using client computer when that client computer has not been used for a period of time, e.g. screen-locking mechanism and need to use login password.

9.6. Application and Information Access Control

The purpose is to prevent unauthorized use of information and information systems.

9.6.1 The information technology group must control the use of information in information systems, including specified access such as the ability to write, read, delete, specified users that have access, checking that authorized information contains data needed to use only.

9.6.2. The accounts of users with special access to information systems such as Root or

Administrator must be assigned to the users as necessary with specified period of access appropriate for working only.

9.6.3 Third parties must express their consent to strictly comply with the Company's policy on information and communication technology security before gaining access to the Company's information technology systems.

9. 6. 4. The information technology department must separate important or high- risk information systems in another area, e.g. separation between the systems connected to the Internet and the Intranet used in the Company, etc.

9.7 Information Technology Access Control

The purpose is to prevent unauthorized access to information.

9.7.1 Access to information files must be controlled and approved as necessary only so as to keep information files secure effectively and separate the users' rights and functions.

9.8 Mobile Computing

The purpose is to control the use of mobile computing including the operations outside the office for security.

9.8.1. The methods must be available to protect data and information assets on portable computers, i.e. Notebook, Palmtops, Laptop and other communication devices; when working off the premises, for example.

- Passwords must be entered to protect all screens.
- Passwords must be entered to protect important information.

Section 10: Information System Acquisition, Development and Maintenance

10. 1 Security Requirements of Information Systems

The purpose is to secure information systems.

10.1.1 The information technology department must determine security requirements clearly in the system to be developed or purchased for use.

10.1.2 The information technology department must analyze information technology systems as to the risks that will corrupt data by focusing on the following parts.

- Preventive measures such as backup
- Measures after damage, e.g. data recovery plan, recovery period

10. 2 Security in Development and Support Processes

The purpose is to secure software for information systems as well as information in the system.

10.2.1 The information system developer must have a process to control modifications to software for information systems actually in use or already available such as

- Requests for modifications must come from authorized persons.
- Requests must be approved by the authority.

10.2.2 The use of software package requires controlling modifications as necessary. Moreover, all changes must be tested and documented to be able to use when updating software in the future.

10.2.3 Contracting to develop the Company's systems must be clear and covering the details of software copyright, system use, system monitoring before installation for the actual use, including system quality certification and determined scope of system development.

Section 11: Creation of username & password and access for ERP (Winspeed)

The information technology department must have written forms for new employee or resignation or transfer of department.

11.1 The information technology department must require filling in the form to request username and password with the following information.

11.1.1 Name -surname of the employee requesting access

11.1.2 Department name by stating new employee, resignation, transfer of department

11.1.3 Specify access grants and the date of request

11.1.4 The signature is required. Consent is given by the heads of accounting and technology departments.

11.1.5 The top module can be accessed only by the system admin. In case other persons need to access the top module shall be approved by the Executives.

11.2 The information technology department must set password strictly for security.

11.2.1 The password must have 8-10 characters long.

11.2.2 The password must start with upper-case, followed by lower-case letters.

11.2.3 The password must have at least 1 number.

11.2.4 The password must be reset every 90 days.

11.3 The information technology department must regularly monitor user and access.

11.3.1. User access must be checked to conformity with HR information every 90 days.

11.4 The information technology department must provide written evidence for updating the form or changing program (erp).

11.4.1 In case of modifications to program or addition of functions by vender,

the accounting department must send a written email to the vender as proof.

11.4.2 Every time of modifying the form requires approval of the authority.

Also, the details of modified form must be collected for storage as evidence.

Section 12: Business Continuity Management

The purposes are to prevent any interruption or disruption to the operations of the Company to protect major work processes of the Company as a result of failure or disaster on information technology systems and to be able to recover the systems in a timely manner.

12.1. The process must be available for the Company's business continuity management.

Also, this process must be adjusted regularly.

12. 2 The process of business continuity management of the Company must be tested regularly.

Section 13: Compliance

13.1 Compliance with Legal Requirements

The purpose is to avoid violations of criminal and civil laws, the Acts, regulations and contracts.

13. 1. 1 The information technology department must study and determine the details of policies, rules, regulations, laws or contracts relating to the use of information technology of the department.

13. 1. 2 All staff members must acknowledge, understand and comply with the details of policies, rules, regulations, laws or contracts relating to the use of information technology strictly.

At least the following items must be available.

- Policy on information and communication technology security
- Computer Offenses Act
- Electronic Transaction Act
- Act on Rules and Procedures for Government Electronic Transactions
- Copyright Act

13. 1. 3 Information generated, stored or transmitted through the Company's information technology systems is considered as the Company's property (except for information that is property of customers or third parties, including software or other materials protected by patents or copyright of third parties). The Company may disclose or use such information as evidence for investigating various offenses with no need to inform the users in advance.

13. 1. 4 For the purpose of managing and maintaining security of information technology systems of the Company, we reserve the right to check the use of computers, computer system

networks of the users to ensure compliance with the policies set forth and access, review and monitor the users' emails without prior notice. However, this inspection will be performed if necessary only. Any information of the users will not be disclosed unless disclosed according to the order of the court, the legal provisions or with consent of the users only.

13.1.5 All staff members are not allowed to use the Company's property and information technology systems in any manner contrary to the laws of the Kingdom of Thailand and international laws in whatever case.

13.1.6 Required compliance with the Copyright rules for using intellectual property provided by the department and need to be careful not to violate the terms of Software Copyright strictly, including control of using software under the copyright granted, that is registration to use software requires storage of copyright ownership proof, regularly checking whether the software installed is correctly copyrighted or not.

13.1.7 The users are not allowed to use, reproduce or distribute any image, song, article, book or document in violation of copyrights or install pirated software on information technology systems of the Company strictly.

13.1.8 In order to ensure that staff does not intentionally or unintentionally infringe copyrights, therefore no software should be copied, which is installed on the Company's computers for any purpose without authorization.

13.2 Information System Audit Considerations

The purpose is to make the entire information system audit have minimal impact on the operations of the department.

13.2.1 The information technology department must plan the entire system audit.

The audit to be performed must have minimal impact on the systems and the operations of the department.

13.2.2 The information technology department must protect software used to audit the system. Software must not be misused or important data must be protected that is the result of audit by such software.

Section 14: The protective measures and mitigate the impact of Cyber Threats

The objective is to protect risks and mitigate the impact of Cyber Threats which is presently found as follows;

Malware - Threats of being attacked by malware (unwanted and harmful program)

Web Application Attack – Threats of being attacked by Web Application

Phishing - the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication

DDoS (**Distributed Denial of Service**) – **DoS** - a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic

Spam - Threats of being attacked by unsolicited bulk email

Botnets - Threats of being attacked by email bombing and spamming or private internet-connected computers whose security has been compromised by malware and under the attacker's control as a DDoS attack. Spam (Violate) (AUP = the Acceptable Use Policy))

Ransomware - a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment

Data Breaches - an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner

The determined the protective measures to protect the information technology systems in business operations from the Cyber Threats as follows;

14.1 Determine the policy and protective measures in order to protect the information technology systems in business operations from possible emerging risks and threats

14.2 Install a Firewall Protection to protect the essential systems

14.3 Install the copyright programs or licensed programs which have regular updates for system protection

14.4 Install virus and spam protection programs that meet the security standards for every user and provide regular update

14.5 Select the email hosting or web hosting who meets the standard and can provide the system service with security control

14.6 Determine the guidelines for the Company's data back-up systematically including the frequency of recovery period which will not affect to the normal business operations. Establish the separated data storages independently to protect threats that may arise from network connections to databases and main working systems

Description to issue and improved the document

Item	Document number	Approved date	Reference the Board of Directors Meeting to approved
1	*CS20180802*	14 August 2018	The Board of Directors Meeting no. 4/2018
2	*CS20180802* (Rev 1)	14 November 2018	The Board of Directors Meeting no. 5/2018
3	*CS20180802* (Rev 2)	13 November 2020	The Board of Directors Meeting no. 4/2020