Prepared by:	Reviewed by:	Approved by:
Mr. Boonmee Warapattanapong **Director** **Information Technology**	**Mr. Santi Bangor** **Chairman** **of Corporate Government Committee**	**Mr. Prasert Bunsumpun** **Chairman** **of Board of Directors**

Preface

Today, our business is increasingly dependent on information technology which leads to information technology risks, such as viruses, intrusion, hacking, etc. In addition, in order to comply with the Computer Crime Act B.E. 2550 the company's information technology resources must be protected for all users.

To protect the company's IT resources, the IT department has formulated the "Information Security Policy" to protect the organization and users against cyber-threat and improper use.

This policy applies to all users of the Company's IT resources, regardless of where they are located. Violators of this policy may face disciplinary and legal consequences.

All users must be responsible for the appropriate and legal usage of the company's IT resources.

Definition

"The Company" refers to Thoresen Thai Agencies Public Company Limited (TTA), Thoresen & Co., (Bangkok) Ltd. (TCB) and Thoresen Shipping Singapore Pte, Ltd. (TSS)

"IT Resources" refers to computer, network, hardware, system or application software, and information systems in electronic format.

"IT Department" refers to TTA's IT department staff who are assigned by the company such as IT Director, System Administrator, and/or System Engineer who will be responsible for system security, policy creation and Hardware and software standard determination for best interests of the company.

"User" refers to all employees, partners, contractors, consultants, temporary employees, and others who have been granted access to IT resources. However, this does not include those who access the Company's systems intended for public use, such as third parties who visit the Company's website.

"Computer" refers to any computer, connecting device, or electronic device that connects to the company network or stores company data, whether or not it belongs to the company, such as a PC, server, mobile phone, tablet, or other electronic devices.

"Company's computer" refer to any computer or electronic device provided by company to users, such as PC, Laptop laptop and tablet.

"Personal computer" refers to any computer and/or electronic equipment that is not owned by company.

"Prohibited information" refers to any form of information, such as e-mail, content uploading, images, clip art, games, music, movies, programs, and file Documents containing the following inappropriate contents

- Deceptive or incorrect information that could create panic or harm to others.
- Embarrass and/or cause harm to others.
- Pornographic content.
- Gambling and drugs.
- The Kingdom of Thailand's security or other terrorist threats, such as malicious threats, false information that could harm the economy and generate panic.
- Malicious hacking, system disruption, or data theft.
- Infringe on any intellectual property or copyright laws.
- And any other improper or unlawful content, such as posting a pornographic URL link or anything that leads to such information showing the aim of distribution.

"Media" refers to an electronic data container, such as a floppy disk, thumb drive, CD, DVD or hard disk (both internal and external) includes a cloud system.

"Confidential Information" and "Proprietary Data" means all information that is not in the public domain, which is by its nature confidential or that has been designated as confidential by the disclosing party and includes but is not limited to trade secrets, know-how, financial information and the data and reports in any electronic file format which related to or exported from the Company's business application databases, e.g. SAP application database, etc.

"Data Loss Prevention System" Event Log means the Cyber Security Software which will be recording the movement of electronic or computer data files on each company provided personal computer to the event log database. This process will be working in the background while the computer running without interrupting the daily routine working of staff.

1. Objective

In order to use the Company's IT resources in the most appropriate manner that poses the least risk and in accordance with applicable laws such as the Computer Crime Act, B.E. 2007.

2. Scope of Enforcement

This policy applies to all users of the Company's IT resources, regardless of location.

3. Responsibilities

Users must perform the following actions.

1) Strictly adhere to this policy and any other relevant policies.
2) Take responsibility for any activity that occurs under the user ID.
3) Inform the IT department of any irregularities such as
    - The Company's computer, data, or any device or storage media containing the Company's data has been lost.
    - Aberrant data content
    - Found a policy violation or improper use

- Believe the password is insecure
- Someone is using your user id without your permission.
- The company's computer exhibit odd symptom, such as slowness and bizarre screens.
- There is an abnormal warning when opening file or receive email which has virus and/or other deceptive features.
- A virus has infected the company's computers.

4) Report any vulnerabilities or weaknesses to the IT Department immediately, such as the notebook being discarded or the anti-virus program not being updated.

4. Authority and Rights of the Company

The Company grants the IT department the authorization to maintain the security of the information systems and the right to perform the following actions:

1) Maintain the system's stability and security within the proper scope. The company reserves the right to examine the company's computer and/or users' improper use. It may be necessary to record, monitor, and/or check files, e-mail, and Internet activities which authorized by the Company's management. Users should not expect privacy when using the Company's computers and other infrastructures.
2) Keep track of computer system and network traffic statistics, such as who visits which websites and when (to comply with Computer Crime Act B.E.2550).
3) Delete or uninstall irrelevant jobs or programs, such as uninstalling non-standard programs, deleting forbidden files, compressing disks for irrelevant data, and remove business irrelevant mail from the queue without prior notice.
4) Standardize system usage, such as file storage limits, the number of e-mail recipients, and the size of e-mail attachment files.
5) Denial of service or restriction if used incorrectly for example blocking website, sending or receiving email from a blacklist domain.
6) Recover files and e-mails for inspection or other purposes, even if these files or e-mails have been deleted

The Company is not liable for the actions or inappropriate content of the user.

5. Information Access Control and Prevention Regulations

5.1 Prohibited Actions

The following actions on IT resources are prohibited without permission, according to Company regulations. It may also be a violation of the Computer Crimes Act BE 2550, which is punishable by both a fine and imprisonment.

1) Disclosure of trade secrets and other confidential information of the company, whether inside or outside the company, without prior written approval from top management.
2) Access to or attempt to get access to IT resources without authority or in excess of the rights granted.
3) Disrupt, destroy, delete, modify, change, add to, or damage IT resources.

4) Dissemination of sensitive security information such as security systems and/or passwords.
5) Perform or attempt hacking, security testing, or any other action that could harm the IT resources.
6) Tracking network traffic or collecting information on the computer, such as keystroke logging or password phishing.
7) Create or distribute "prohibited information" in any form including chat, upload/download, email, or posting on the Internet.
8) Threatening, offending, harassing, or causing harm to others, such as photo editing that will cause dishonor, suffer as a result of being insulted or shamed.
9) Any acts that are against the law and/or the company's regulations.

5.2 User ID and Password

1) To prevent hacking, users must log-off, lock the screen, or turn off the computer when not in use.
2) It is forbidden to share User ID and password with the exception of permission from IT department in accordance with the company's regulations
3) It is strictly forbidden to disclose your and other users' user IDs and passwords for accessing the company's IT resources with third parties.
4) Users are only permitted to use systems in accordance with the rights granted.
5) If user thinks the password is leaked or someone else knows it, user must report to the IT department for investigation and user must change the password immediately.
6) In order to resolve computer problem, user may be required to share password to IT Department, and user must change password immediately after the problem has been resolved.
7) Password setting rules
   - Passwords should be at least 8 characters long and include numbers or special characters like # $ @!
   - Avoiding to set passwords that are easily guessable, such as birthdays, dictionary words, or well-known words.
   - User will be forced by the system to change passwords every 90 days otherwise user will not be able to access the system
   - Password must be set or changed by user's owner.
   - Password should not be shared, written down, or stored in places where others can see.
   - Password never expire will be granted for specific user, shared user and Top Management whom IT Dept. confident that there is not any impact to system security.

5.3 Virus Protection

1) Computers connected to company network must have an anti-virus program installed that has been approved by IT department.
2) Computer that connects to company's network or system must first be checked by IT Department.
3) Antivirus software that has been installed must be updated regularly and functional.
4) At the request of IT department, the user must perform virus scanning on any file recording immediately in order to control the suspicion of malware.
5) Anti-virus software must be continually monitored and updated by user who use company's laptop.

6) It is prohibited to disable, change, or remove anti-virus and security tools installed unless authorized by the IT department according to the company's policies.

5.4 Company's Network Terms of Use

1) Use Company's network and Internet for business-related purposes only.
2) Never connect a personal device to a company network without the approval of the IT department.
3) Do not connect the company's network or internal systems to an external network such as modem over the phone or ADSL connection unless authorized by the IT department.
4) Due to the possibility of network traffic tracking, company or customer data must be encrypted before being sent to the outside via email, FTP, or chat.
5) Changing internal network connections by the user is prohibited, such as connecting to an external device, without the consent of the IT department.
6) Outsiders are strictly prohibited from connecting to and using the company's network infrastructure to access to the server, with the exception of Internet access only (Internet Terms of Use 5.6).

5.5 E-Mail Terms of Use

1) Avoid sending sensitive company information, customers or employee information over email without encryption (since it may be intercepted). The level of information confidentiality is determined by department's head.
2) It is forbidden to use email for the following purposes:
   - Sending "Prohibited information"
   - Sending e-mail from another user's account without owner's consent.
   - Sending e-mail without sender's name by using any method to conceal sender's identity (anonymous).
   - Sending e-mails that are unrelated to the Company's business or solicit political, religious, or other actions that may offend or hurt the recipient.
   - Send threatening, intimidating, or privacy-invading e-mail to others.
   - Sending too many e-mails about personal matters, such as sending very large files or many recipients.
3) Check the recipient's e-mail address before sending. Also make certain that the email size does not exceed the size specified in the policy.
4) Department Head has the right to inspect the content of user's mail under his/her command. This must be requested through IT department.
5) When user receive unsolicited e-mail (Spam), such as advertising mail, junk mail, or fraudulent mail. User should not respond, click links, interact with, or forward that email and should notify IT department to have that e-mail address blocked.
6) Attached file
   - Avoid opening file that appears to be an exe file, script file, or zip file when receiving an e-mail from an unknown sender or if the file is found to be suspicious.

- It is necessary to scan files for viruses before to delivering them to avoid infecting others' computers by delivering malicious data

7) Only certain departments, such as Corporate Communications, have the ability to send e-mail to all users. Communications with all employees must go through this department only.

5.6 Internet Terms of Use

1) Must access through security system installed by IT department only, such as Firewall, Proxy Server.
2) Prohibit visiting websites rated as a security risk, adult/mature content, gambling, and bandwidth-consuming
3) Downloading programs or software from the internet is prohibited, regardless of whether they are used at work unless authorized by the IT department.
4) Use the Internet only when it is necessary. It should not be used to download movies, listen to music, or watch television online. It obstructs work and lowers productivity. It also adds to the network's traffic load.
5) Do not use the Internet to download/upload, send message or content that related to
   - Intent to load "forbidden information".
   - Information about the company's business, especially uploading to a private cloud.
   - Illegal and/or against company's policy.
6) If the user is the third party, they must present their name, ID card number, and company to the IT department in order to be authorized to access the Internet in accordance with the IT department's regulations, and they must strictly adhere to the internet terms of use.

5.7 Remote Access Terms of Use

1) Remote access is not granted to the user as a general rights. The user must request and receive approval from Department Head as well as IT Department.
2) Remote access to internal IT resources must be done only through a VPN which specified by IT Department. Other remote access software, such as team viewer, anydesk, or any other software, must be authorized by IT department and restricted for specific user only.
3) IT departments may consider to stop providing remote access services temporarily when improper access or misuse is detected.
4) While connecting to VPN, user must proceed with caution and disconnect or turn off the computer when not in use.

5.8 Company's Computer Terms of Use

1) Important business data should not be kept on a desktop or laptop computer. It must be saved on the Company's central drive designated by the IT department.
2) Computer which stored important Company information while using that information. When finish, user must transfer it to central drive and delete it from desktop or laptop computer.
3) Do not store "Prohibited Information" on company's computer.
4) Do not store non-business-related information on company's central drive.

5) Do not relocate company's computer. Except with the permission of IT and Administration Department.

6) User is responsible for safeguarding the Company's computer and using it with caution, such as keeping a portable computer with you at all times or keeping it in a secure location while you are away to prevent espionage.

7) In order to repair, claim, discard or donate the company's computer, the user must take it to the IT Department for backup or cleanup of the disk and other recording media, as recommended by the IT Department.

5.9 Software Terms of Use

1) Installing programs or software other than those specified in Standard Software considered by the IT Department on Company's computer is not permitted unless authorized by the IT Department.

2) Programs or software installed on the Company's computer must be legal and have a valid license.

3) It is not permitted to install Company's program or software on any other computer or device that is not owned by the company.

5.10 Storage Media Terms of Use

1) All "Confidential Information" and "Proprietary Data" should be stored in the central drive of the department with access restricted to the only authorized person. For that information that previously stored in any media, it should be kept as confidential in a secured area and restricted to the authorized person in order to prevent loss and unauthorized use of information. And company has the right to monitor and record the movement of the "Confidential Information" and "Proprietary Data" into the "Data Loss Prevention" system log for further verifying and auditing.

2) Do not keep "forbidden information" on company storage media.

3) If storage media contains confidential information, it must be kept secure such as in a safe, or lockable drawer.

4) In order to repair, claim, discard or donate storage media. It is the user's responsibility to take it to IT Department for backup or cleanup.

5) Storage media from outside must be inspected by IT Department before connecting to the company's computer

6. Policy Violation or non-compliance

Any violation of this policy will be treated as a serious violation of the Company's regulations.

If a policy violation is discovered, IT department will take the following steps:

- 1st notify the supervisor verbally or via e-mail.
- 2nd sending notification directly to user with a copy to supervisor
- 3rd sending second notification to user and a copy to supervisor and inform Human Resources Department for disciplinary action.

In case of a clear and serious violation (even if it's the first time), IT Department and Human Resources Department will inform senior management which could result in disciplinary action as well as legal action, such as the Computer Crimes Act B.E.2550 which imposes both prison and fines (up to 20 years imprisonment.)

7. Exemption

In some circumstances, there are sufficient reasons to deviate from the policy. Users must request to the IT department for an exception to this policy and be considered as non-serious case. This proposal must be agreed and approved by the Department Head.

8. Backup and Disaster Recovery

The IT department is directly responsible for preparing the appropriate backup system in accordance with the Backup and Recovery Best Practice standard. IT department will determine the scope, storage media (media) to keep backup data, backup frequency, and data replication to the DR Site which is part of the Backup and Disaster Recovery Procedure.

9. Audit and Risk Assessment

IT department must cooperate with relevant department to setup an audit and assessment of information technology management that includes risk assessment and the risk control to be within the acceptable level of the Company. And appointing a person in charge of information technology risk management, to ensure that information technology risk management is properly managed.

10. Personal Data Privacy Policy

The Company has no policy to store personal information for commercial or other purposes. Only necessary data is stored and must be consented to.

11. Policy Review

Because of the rapid pace of information technology, the IT Department should evaluate this policy at least once a year to verify that it is up to date and does not compromise system security.

REVISION RECORD			
Version No.	**Date** (dd/mm/yyyy)	**Created/ Modified by**	**Description and Reason for Changes**
Issue 01, Rev. 02	26/11/2014	Information Technology	Revised to reflect current operations.
Issue 01, Rev. 03	11/11/2021	Information Technology	Revised to reflect current situation.

Appendix A – Standard Software

Server	Microsoft Windows Server 2008, 20013, 2016
Client	Microsoft Windows 7, 8, 10
Office Suit	Microsoft Office 2010, 2013
Mail	Microsoft Exchange 2010
Anti-Virus	Sophos
Client Management	Starcat
PDF Reader	Adobe PDF Reader
Zip File	7Zip, WinZip, WinRar
AD Management	AD Manager Plus
AD Audit	AD Audit Plus
Online Meeting	Microsoft Teams
Remote Control	Anydesk, Team Viewer
VPN Connection	FortiGate Cilent VPN
ERP System	SAP Business
Backup Software	Veritas and Veeam