INFORMATION TECHNOLOGY SECURITY POLICY

EUROASIA TOTAL LOGISTICS PUBLIC COMPANY LIMITED

REVISION 4

EFFECTIVE DATE 20 FEBRUARY 2025

Preparation and Approval History

Document No.	Editor/Controller	Reviewer	Approver
CP-BOD-024-02	Managing Director	Chief Executive Officer	Board of Directors
	3 January 2025	30 January 2025	20 February 2025

Revision History

Revision	Revision Date	Effective Date	Revision details
1	10 October 2021	9 November 2021	First issue
2	5 January 2022	19 February 2022	Adding Data Classification Procedures
3	10 June 2022	6 August 2022	Revise company name after conversion to public limited company
4	3 January 2025	20 February 2025	Annual review

Note: To add or cancel any document, proceed according to the acts set out in the Approval and Implementation Authority.

Information Technology Security Policy

To enable the information technology system, network system and computers of Euroasia Total Logistics Public Company Limited (**"Company"**) and its subsidiaries to use the information system, network system and computers appropriately; have security and support the company's operations continuously; use the systems properly consistent with the requirements of the Computer Crime Act and other applicable laws as well as preventing threats that may cause damage to the company, the company has established the Information Technology Security Policy as follows:

Definition

The definitions in this section are meanings for terms used in this Information Technology Security Policy to have clear meaning and the same understanding.

1. **"Company"** means Euroasia Total Logistics Public Company Limited and its subsidiaries that use the information system, network system, and computers together.
2. "**Department of Human Resources**" means the company's Department of Human Resources overseeing human resource management.
3. "**Department of Information Technology**" means the Department of Information Technology of the company.
4. "**Users**" means directors, executives, operators, and authorized external users to access the company's network system.
5. "**Worker**" means an officer or employee of the company.
6. "**External user**" means a person or a juristic person who is a contractual party of the company who carries out activities within the company.
7. "**System administrator**" means an Information technology manager or other operators who are responsible for development, editing, update, and maintenance of the information system and network system used in the company or departments having duties and responsibilities for maintaining the information system and network system directly.
8. "**Information**" means facts obtained from information taken through the processing and organization that may be in the form of numbers, texts, documents, diagrams, maps, photographs, films, photo recordings, sound recordings, recording by computer, or graphics into a system that users can easily understand and can be used for management, planning, decision making, etc.

9. “**Information System**” means the company’s work system that is used to store, process, and disseminate data that works in conjunction with hardware, software, data users, and processing to create information that can be used for planning administration and supporting the company’s working mechanism.
10. “**Network System**” means a system that can be used to communicate or transmit data and information between various information technology systems of the company, such as LAN, wireless, intranet, internet, and other communication systems.
11. “**Assets**” means any tangible and intangible assets or things that have value to the company including information, information system, and information technology and communication assets, such as personnel, hardware, software, computers, computer servers, information system, network system, network equipment, IP address, or licensed software.
12. “**Information Technology Security**” means security and safety for information technology and network systems of the company by keeping confidentiality, integrity, and availability of information, including other properties, namely authenticity, accountability, prohibition, non-repudiation, and reliability.
13. “**User’s Rights**” means the levels of access to data of users and external users including general rights, specific rights, and any other rights related to the company’s information system and network system.
14. “**Access to or Control of the Use of Information**” means permission, assignment of rights, or authorizing users to access or use the network system or information system, both electronically and physically, as well as stipulating rules on unlawful access.
15. “**User Account**” means a username and password for users and external users.
16. “**Security Incident**” means a case that specifies an incident, condition of the service or network that shows the possibility that there will be a violation of the information technology security policy or failure of preventive measures or events that may not be known to be related to security.
17. “**Adverse or Unexpected Security Situation**” means a situation which may make the company’s systems compromised or attacked and its security is threatened.
18. “**Encryption**” means bringing data to be encrypted to prevent others from hacking into the data for use. People who can open the encrypted data need a decryption program to restore the data for normal use.
19. “**Authentication**” means the security procedure for accessing the system. It is a procedure to verify the identity of the general system user. It is proven by using a username and password.
20. “**SSL (Secure Socket Layer)**” means data encryption technology to increase the security of communication or transmitting information on the internet network between a server and a web browser or a used application.

21. “**VPN (Virtual Private Network)**” means a network of virtual personal computers using real data transmittal. The transmittal is encrypted exclusively through the internet network, making it impossible to read and invisible to others until it reaches to the destination.

Section 1 Governance of Enterprise IT

The Information Technology Governance aims to ensure that the company is able to achieve its goals by adopting information technology as a means of support and effectively managing risks that may arise from the effective application of information technology. Good information technology management requires a link between information technology management process and powerful resources and information to support appropriate policies, strategies, organizational goals and risk management, including reporting and monitoring the implementation to ensure that the technology the company has used can support strategies, achieve business objectives, and build competitiveness as well as adding value to the company. The company must consider taking at least the following actions:

1. IT Security Policy

1.1 The company must have a duty to supervise the formulation of a written information technology security policy and communicate such policy in order to understand and comply with it properly, especially between the information technology department and other departments within the company for coordination and business operations to achieve the set goals.

1.2 The company must provide a regular review of the information technology security policy or when there is a change that affects the information technology security of the company.

2. IT Risk Management

It must be consistent with the corporate risk management policy and cover the following matters:

2.1 The determination of duties and responsibilities in management and risk management on information technology, IT officers are responsible for studying and providing methods or guidelines on information technology to mitigate risks or manage existing risks and presenting them to the management team for consideration of the information technology risk management.

2.2 The identification of information technology related risk should cover major risks, such as

2.2.1 Risk from personnel

2.2.2 Risk from software and data

2.2.3 Risk from the network system and internet

2.2.4 Risk from the hardware and computer equipment

2.2.5 Financial risk

2.2.6 Risk from flood and storm

2.2.7 Risk from earthquake and building collapse

2.2.8 Risk from fire

2.2.9 Risk from theft

2.2.10 Risk from power failure

2.3 The determination of methods or tools for managing risks must be at an acceptable level, and then the company prepares a table of description of risk by having the heading, risk name, type of risk, characteristics of risk, risk factors, and impacts, etc. The company also determines the levels of the opportunity of an incident and the severity of the risk impact, including a risk map.

2.4 The information technology risk indicators must be determined, including tracking and reporting results of the indicators to responsible persons in order to manage risks properly and timely.

Section 2 IT Security

1. Additional guidelines for the information security policy and measures

Objective

To prevent violations of the information technology security policy

Guidelines

1.1 Do not use resources and computer networks to act illegally and contrary to the good morals of society, such as creating a website for trading or disseminating anything that is illegal or against good morals.

1.2 Do not access to use the network computers or computers with another user's account name, both authorized and unauthorized by the owner of the user account name.

1.3 Do not access the computer system and data protected from other people's access to edit, delete, add, or copy.

1.4 Do not distribute other people's information or that of the organization without permission from the data owner.

1.5 Do not harass, obstruct, or damage the company's resources and computer network, such as sending computer viruses, or downloading a program causing denial of service of a computer or network devices. 1.6 Do not smuggle to receive data in a process of receiving and sending in the company's computer network and that of others.

1.7 Before using any portable recording media or opening files attached to electronic mail or files downloaded from the internet, they must be checked for viruses by an antivirus program first all the times.

1.8 Users must not allow others to share their username and password to access their computer.

2. Organization of Information Security

Objective

To define the security management framework of information system within the company.

Guidelines

2.1 Senior executives are responsible for overseeing security to comply with the company's information technology security policy.

2.2 The Head of Information Technology Department must assign duties to operators in the department responsible for maintaining the security of the information system and control operations in order to maintain the company's information technology security policy.

2.3 The Head of Information Technology Department is responsible for managing, supervising, monitoring, and reviewing the overall information technology security policy of the company.

2.4 Information Technology operators assigned as system administrators for that system must be responsible for checking and monitoring the safety of the use of the system. When there is an adverse or unexpected security situation, they must implement corrective actions and report to the supervisor.

2.5 Users and internal and external agencies must be responsible for complying with the company's policies and practices in maintaining the security of the company's information system and not commit any violation of the law related to computer-related offenses.

3. Human Resource Security

Objective

To enable users to understand the policies, duties, and responsibilities of using the company's information system.

Guidelines

3.1 It must define in writing the duties and responsibilities of information system security for persons or external agencies hired to work and must be consistent with the company's information technology security policy.

3.2 There must be an agreement signed between the user and the agency that the company's secrets will not be disclosed (Non-Disclosure Agreement: NDA). The signing will be a part of the employment of that user, provided that it is binding both while working and for a consecutive period of not less than 1 year after its termination.

3.3 To ensure the most accurate and up-to-date management of user accounts, the Department of Human Resources or relevant departments must notify the Information Technology Officer immediately in any of the following circumstances:

3.3.1 Employment

3.3.2 Changes in employment condition

3.3.3 Resignation from employment or the termination of being a director and user of the company

3.3.4 Relocation of department

3.4 Users and external agencies hired to work at the company must be informed of the policies related to the information technology security.

3.5 New employees of the company must be trained on information technology security policy. This should be part of the orientation.

3.6 After a change or termination of employment or the termination of the project, an access to information in the information system must be terminated immediately.

4. Computer and Peripheral Access Control

Objective

To make users aware of the duties and responsibilities in the use of computers and computer equipment of the company, including understanding and strictly following to protect the company's resources and information to be safe, accurate and always available.

Guidelines

4.1 The users of the company's computers and computer equipment must be responsible for the assets used.

4.2 The company's computers and computer networks are forbidden from operating any commerce or service for personal and inappropriate purposes.

4.3 The users are not allowed to install and modify the programs on the company's computers, unless consulted or advised by a system administrator or authorized by the highest authority of a department.

4.4 The modification of computer components and peripheral equipment is prohibited, unless approved by a system administrator or the responsible department. The users must maintain the condition of the computer and peripheral equipment to be in the original condition.

4.5 The users must not store or use computer equipment in hot, dusty places and must be careful about impacts.

4.6 Do not use or place all kinds of computer equipment near liquids, magnetic field, high voltage, in the place with vibrations, and in environments with temperatures above 35 degrees Celsius.

4.7 Moving computer equipment should be done with caution. Do not place heavy objects on top of it or throw it.

4.8 Do not move the computer while the hard disk drive is in operation or while it is in use.

4.9 Avoid hard objects touching the computer screen that could scratch or break it. Wipe the computer screen as gently as possible and wipe in the same direction. Do not wipe in swirls because it can scratch the screen.

4.10 The terminated users or those at the end of a project must return all responsible computers and computer equipment to the responsible department in a ready-to-use condition.

4.11 When moving computer equipment for work outside the office, the users must comply with the requirements about taking the company's assets out of the company.

4.12 The users are responsible for preventing loss. Do not leave the device in a public place or areas that are at risk of loss.

5. Control of the Use of Computer Programs (Software License)

Objective

To make users aware of their duties and responsibilities in using computer programs as well as understanding the use of licensed programs and strictly following the guidelines, including the use of computer programs to be secure and in accordance with the Computer Crime Act and related laws.

Guidelines

5.1 System Administrators' Requirements

5.1.1 Be responsible for controlling and supervising the use of computer programs as well as allocating the use within the company according to the specified licenses.

5.1.2 Be responsible for installing and upgrading computer programs for users on the scheduled dates and times.

5.1.3 Remove and terminate the license to use the computer program immediately when the company and/or department notify the termination and/or transfer of the license to use the computer program.

5.2 Users' Requirements

5.2.1 Users must use a computer program such as a wise man would use their own property without using it in an illegal way or in violation of the law for another person that causes damage to the company.

5.2.2 The programs installed on the company's computers are legitimate licensed programs. Therefore, users are prohibited from copying programs and installing them on their computers or modifying or giving them for others to use.

5.2.3 Users are prohibited from copying, selling or distributing violated programs and sets of created commands without permission, especially used as a tool to commit illegal offenses.

5.2.4 Unlawful computer programs are strictly prohibited to be installed on the company's computers. In the event that the user brings any other computer program other than the company's programs to use on the computer system, regardless of whether there is a licensed software or freeware, if there is damage or infringement occurs, the user must be solely responsible.

5.2.5 Users must notify an authorized person of installation, termination of use, transfer, and return of computers and computer programs for approval. An administrator of the information technology system is responsible for implementing as approved in each case.

6. Information Asset Control and Access to Computer System

Objective

To keep information assets from being vulnerable to unauthorized access while the device is not being used by users.

Guidelines

6.1 The information assets, such as documents, data recording media, computers, and data must be controlled from a state of vulnerability to unauthorized access while the device is not being used, and users are required to log out of the information system when idle as follows:

6.1.1 Log out of the information system immediately upon completion of the work.

6.1.2 The computers must be protected by using appropriate authentication before accessing it.

6.1.3 The critical information of departments must be stored and backed up in a safe place. Users' data can be stored in the following formats:

(a) In the database of that Application system stored within the company's Data Center. Exporting data from the Application system cannot be performed.

(b) The data can be stored in a shared file (central drive) in a folder granted permission.

6.1.4 Turn off the computer when finishing daily work, unless it is a server computer, which must be used 24 hours.

6.1.5 Set the screen saver on the computer to automatically lock the screen after 10 minutes of inactivity.

6.1.6 Request for approval from the highest authority of a department or above in the case of wanting to bring information assets, for example, documents, storage recording media, or computer equipment, out of the company every time by complying with the requirements for taking the company's assets outside.

6.1.7 Be careful and take care of the company's assets as users' own property. If lost by negligence, users must be responsible or indemnify that damage.

6.1.8 Put tags on computer equipment and computers, which are assets of the company.

7. Use of Electronic Mail

Objective

To make the transmission of electronic mail support the operation properly, accurately, conveniently, rapidly, timely, efficiently, and safely under the requirements of the law, rules, regulations, and the company's information security measures as well as in order for users to understand the importance and be aware of problems arising from the use of electronic mail service on the internet network, users must understand the rules defined by the administrator. Users shall not infringe any rights or take any action that will create problems or disregard the rules specified and must strictly comply with the administrator's suggestions.

Guidelines

7.1 Users of the electronic mail service must not commit a violation of the Computer-Related Crime Act, Electronic Transactions Act, relevant laws, and policies and requirements related to information technology set by the company.

7.2 Departments or users of the company's electronic mail service must use the service for the benefit of the company.

7.3 Users will be granted the right to use the electronic mail service provided that the administrator registers the electronic mail service users according to the list of users notified by the Human Resource Department.

7.4 Do not use the e-mail address of others for reading or sending and receiving messages.

7.5 When using the electronic mail, users must not falsify the sender's account name or another user account.

7.6 For sending electronic mail to service recipients according to the company's mission, users must use the company's electronic mail system only. The use of other electronic mail systems is prohibited, except in the event that the company's electronic mail system is disrupted and must have permission from the supervisor only.

7.7 In electronic mail, polite language is required. It must not be contrary to good morals, incite, provoke, insult, or imply unlawful ways. Users must not send messages that are personal opinions claiming to be the opinion of the company or causing damage to the company.

7.8 Do not use the company's electronic mail system to disseminate information, text, pictures, or anything else that looks contrary to good morals, national security, laws, lese-majesty, or affects the company's operations as well as disturbing other users and service recipients of the company.

7.9 Users are prohibited from bringing electronic mail addresses to use in personal affairs, such as personal business, and application for social networks. If such actions are detected, the e-mail owner or the service user shall be liable for such action.

7.10 Do not take an action that will cause problems in the use of system resources, such as creating chain mail, sending spam mail, letter bomb, or letters for spreading viruses.

7.11 Do not transmit the company's confidential information to other persons or agencies that are not related to the company's mission.

7.12 The transmission of the company's confidential information should be encrypted.

7.13 After using the electronic mail system, users should log out of the system every time.

7.14 In case of receiving complaints, requests, or finding unlawful grounds, the company reserves the right to terminate or temporarily suspend the service to that user in order to investigate and verify the cause.

7.15 If the service user finds an inappropriate action or one that falls into the scope of an offense occurring in the company, the user must report to the Managing Director by e-mail krishavan@etlgps.com

8. Access Control to Information and Information System and Use of Network System of the Company

Objective

To set measures for using the internet through the company's network system for efficiency and security and to make users aware of the use of websites through the company's network system.

Guidelines

8.1 The Department of Information Technology must define a route of the network connection for accessing the internet through a security system, such as Firewall or Proxy.

8.2 The company's computers must have an anti-virus program installed and cover vulnerabilities of the operating system before connecting to the network system.

8.3 After using the internet, users must close the web browser to prevent an access by another person.

8.4 Users must access sources of information according to the rights granted in accordance with their responsibilities for the efficiency of the company's network system and security.

8.5 Users are prohibited from disclosing important confidential information of the company, except compliance with the company's official disclosure rules.

8.6 Users must be careful about downloading programs of the internet, including downloads to improve

programs that must not infringe any copyright or intellectual property.

8.7 Users are responsible for verifying the accuracy and reliability of computer information contained on the internet before using it.

8.8 Users must not use the company's internet network for the benefit of personal business and enter inappropriate websites, such as websites contrary to good morals, containing contents threating to national security, religion, and monarchy; harmful to society, and pornographic websites.

8.9 Users must use the internet in a manner that is not an infringement of other persons and not cause damage to the company. They are also strictly prohibited to commit any act that is considered an offense under the Computer-Related Offense Act or relevant laws. However, for using the internet for the company's operations in all cases, users must strictly follow the procedures stipulated by the company.

9. Cryptographic Control

Objective

To control unrelated persons from accessing, knowing, or modifying information or operation of the information system in parts that are not related to their powers and duties.

Guidelines

9.1 Data Management

9.1.1 There must be a confidentiality hierarchy. Data needs to be categorized according to its mission and prioritization. It must have determination of means to manage each type of data, including establishing procedures for dealing with confidential or critical information before cancellation or re-use.

9.1.2 The transmission of important data through public networks must be encrypted with an international standard, such as using SSL (Secure Socket Layer), VPN (Virtual Private Network).

9.1.3 It must have measures to control the accuracy of stored data (Storage), input data, processing

(Operate), and display (Output). In case related data is stored in multiple locations (Distributed Database) or sets of related data are stored, it must have a control to make information accurate, complete, and consistent.

9.1.4 It should have data security measures if a computer is taken outside the company's premises, such as repairs, or the stored data in the storage must be destroyed first.

9.1.5 Data Classification Procedures

Data Classification	Features	Examples	Level of Protection
Very confidential data	- Organizational significance very high level - Loss of data or unauthorized disclosure will have damage to the organization at very high level - Related to the strategic plan and key directions for business operations - Need to have a strict measure to control dissemination of information with careful consideration of the list of authorized users	- A merger plan, investment strategy, marketing strategy - A business plan and business direction	Must protect data to be accessed only by authorized persons (Highest Security level)
Confidential Data	- Has importance to the organization at a high level - If data is lost or disclosed without authorization, it will have damage to the organization. - Related to the direction of the organization's operations (effective for a period of time) - Need to have a strict control measure on dissemination of information by limiting	- Information about income, cost, profits, or other financial information - Action plan - Information about customers and business partners - Employee personal information - Password of key users - Network Diagram	Must protect data from access by third parties and unauthorized persons (High Security Level)

	access to certain groups of people only and to be properly protected		
Internal use Data	- Business information, information for internal use and is not allowed to be used outside the organization – If the data is lost or disclosed without authorization, it will have a low level of damage to the organization.	- Rules and regulations - Operational Manual - Standard Operating Procedures	Must protect data from access by third parties (Normal Security Level)
Public Data	- Information that does not require special security protection - Information for public through appropriate channels that have been approved by the organization	- Information that has been published through the website - Information from press releases or regular reports that have been published to the public	Protect only the accuracy and completeness of the information

9.2 User Privilege Control

9.2.1 It must have a control of access to data and data processing equipment by taking into account the use and security in the use of information systems. There is establishment of rules about granting access and the rights for users of all levels to know, understand, and be able to strictly follow the guidelines and realize the importance of maintaining the security of the information system.

9.2.2 It must have assignment of the rights to use data and the information system, such as the rights to use the application system or the internet, to users according to their duties and responsibilities, provided that only the rights necessary for the performance of duties and the written approval of the authorized person shall be granted, including reviewing such rights regularly.

9.2.3 In case it is necessary to use privileged users, it must have a strict control over their use. For considering the extent of control of such users, the company will use the following factors for consideration.

(a) should be approved by the competent authority

(b) should strictly control the use of users with special privileges, for example, limit their use to only if necessary

(c) should determine the period of use and discontinue immediately after such period.

(d) Passwords should be changed strictly, for example, every time after the need for use, or if it is necessary to use it for a long time, the password should be changed every 2 months, etc.

9.2.4 In the event that there is no work in front of the computer, it must have a measure to prevent the use by other people who do not have the rights and duties involved, such as requiring users to log out of the system during the time they are not working in front of the computer, etc.

9.2.5 In the event that it is necessary for the user who is the owner of the sensitive data to grant other users the right to access or modify their own data, such as sharing files. It must be granted individually or to groups only and must cancel such permission if it is no longer necessary and the data owner must have proof of such authorization and must determine the duration of use and suspend the use immediately after the expiration of such period.

9.2.6 In the event that it is necessary to grant the rights to other persons to have the right to use the information system and network system in an emergency or temporary situation, there must be a procedure or work instruction and approval from the authorized person must be sought every time. It must have a record of reasons and necessities, including the need to determine the duration of use and suspend the use immediately after the expiration of such period.

9.3 Control of the Use of User Accounts and Passwords

9.3.1 It must have a system of identification and authentication of users before entering into the sufficiently strong information system, such as specifying a password that is difficult to guess, and must specify that each user have his or her own User Account. In considering whether determining a password is difficult to guess and to control the use of the password is strong or not, the company will take the following factors into account.

(a) The password should be of reasonable length. Most international standards recommend a minimum length of 8 characters (Alphabet + Numeric).

(b) It should use special characters, such as <>$@#.

(c) Passwords should be changed at least every 2 months.

(d) For each password change, a new password should not be assigned by repeating the last 3 passwords.

(e) Passwords should not be assigned in a pattern or easily guessed, such as “abcdef,” “aaaaaa,” “123456,” “password,” “P@ssword.”

(f) Passwords should not be set in relation to the user, for example, name, surname, date of birth, or address.

(g) Passwords should not be defined as words in a dictionary.

(h) It should have the number of times that the user is allowed to enter the wrong password (Logon Attempt – Retries), which is generally 5 times. If entering the wrong password according to the specified number of times, the system or program will not allow or suspend the use.

(i) Passwords should be delivered to users with a strong and safe method, such as a sealed envelope.

(j) Users who receive the password for the first time (Default Password) or receive a new password should change it immediately.

(k) The user should keep the password secret. Do not write it down on paper and attach it to the front of the computer. If the password has become known to others, the user should change it immediately.

(l) In the case of shared user licenses, the administrator will send an e-mail notifying the responsible person to change the password to log into the system when there is a change in the user in the department.

9.3.2 It must have an encryption system for the file storing passwords to prevent it from being known or modified.

9.3.3 It must have a regular check for the list of users of important systems and examine the list of users who do not have permission to use the systems, for example, the list of users resigned or attached to the system (Default User), and suspend their use immediately when detected, such as setting 'Disable', deleting from the systems, or changing the password.

10. Physical and Environmental Security

Objective

An access control in the Data Center Room is intended to prevent persons without authority and related duties from accessing, knowing, altering, or causing damage to data and computer systems. The damage prevention is aimed to prevent data and computer systems from being damaged by environmental factors or disasters. Its content covers guidelines about access control of the Data Center Room and various damage prevention systems that the company should provide within the Data Center Room.

Guidelines

10.1 Control of Data Center Room

10.1.1 Important computer equipment, such as servers and networking devices, must be stored in Data Center Room or a restricted area and the access rights to Data Center Room must be assigned to only those who have relevant duties, for instance, system administrators.

10.1.2 In case a person not having a regular relevant duty may be required to access to Data Center Room sometimes, it requires a tight control, for example, assigning system administrators and/or related users to monitor the performance at all times.

10.1.3 There must be a system to keep records of access to the Data Center Room. Such records must contain details about the person and the time of entry and exit and should be regularly inspected.

10.1.4 The Data Center Room should be divided into proportions, for example, Network Zone, Server Zone, UPS Zone, Battery UPS Zone, to facilitate the operation and make the access control of important computer equipment more efficient.

10.2 Damage Prevention

10.2.1 Fire Protection System

(a) It must have fire alarm devices to prevent or suppress fire promptly.

(b) Main Data Center Room must have fire extinguishers to be used for initial firefighting.

(c) Power failure protection system.

(d) It must have a system to prevent the computers from being damaged by the instability of electricity.

(e) It must have a backup power system for critical computer systems and computer networks to ensure continuity of operation.

(f) Temperature and humidity control system.

(g) The environment must be controlled to have an appropriate temperature and humidity. The air conditioner temperature and humidity value should be properly fixed according to the specification of the computer system because it may malfunction under improper temperature or humidity condition.

11. Maintenance of Operations Security related to Information System (Operations Security)

Objective

To operate with the company's information system correctly and securely, to prevent data loss, and to protect the system from malicious programs.

Guidelines

11.1 Prepare manuals or work instructions related to the company's important information systems to prevent errors in information operations.

11.2 Determine a control for changes in information, such as requesting approval from supervisors before proceeding.

11.3 The information must be backed up before changing information.

11.4 It should have a checking and monitoring system installed to monitor resources of the information systems, for example, CPU, memory, and hard disk, to check whether they are sufficient or not. The data obtained from the system will be used in planning to increase or decrease resources in the future.

11.5 The development system of high-priority systems should be separated from the actual service system to prevent unauthorized changes of information.

11.6 It must have a survey of data, prioritization, determination of data to be backed up, and the backup frequency.

11.7 The high-priority data must have a high backup frequency and should be backed up outside the company.

11.8 The backup system availability must be tested at least once a year.

11.9 There must be measures to prevent malicious programs, for example:

(a) Before connecting to the company's network, personal computers or personal portable computers must install an anti-virus program and cover vulnerabilities of the operating system and web browsers.

(b) Users are required to update the operating system and the used programs regularly, which can be downloaded from the product owner's website to fix vulnerabilities.

(c) When sending and receiving computer data via e-mail, it must be checked for viruses by an anti-virus program before transmission.

(d) Users must install software provided by the company. If they want to install software other than those provided by the company, they must notify the Information Technology Department for a safety check before installation.

12. Maintenance of Communication Security via Computer Network System (Communications Security)

Objective

To prevent information in the network from people, viruses, including malicious code, from accessing or damaging to information or the operation of information systems.

Guidelines

12.1 Network Security Management

(a) Determine network access control to ensure security

(b) Allocate networks between internal and external users contacting the company.

12.2 Information Transfer

(a) An agreement on information transfer must be prepared with regard for the security of information and the system administrator must control that implementation to be safe in all three aspects, namely confidentiality, accuracy of information (Integrity), and readiness to provide services (Availability).

(b) A non-disclosure agreement (NDA) must be signed between the company and an external entity to ensure that the company's confidential information will not be disclosed.

(c) It must have a measure to monitor and examine the performance and quality of services of external service providers to ensure that it is in accordance with the contract and agreement.

13. System Acquisition, Development and Maintenance

Objective

The control of development or modification of the information system are intended to make the computer system developed or modified have the accurate and complete processing system and meet the needs of users. This is to reduce the integrity risk. The content covers the process of development or modification from the beginning, including a request, until the actual use of the developed or modified system.

Guidelines

13.1 There should be a written procedure or work instruction for developing or modifying the work system. It should have at least requirements on processes of requesting, developing or modifying, testing, and transferring the work system.

13.2 It should have a procedure or work instruction for a change in the computer system in case of emergency (Emergency Change) and a record of reasons and necessities and seek approval from the authorized person every time.

13.3 The details of the said procedures should be communicated to users and persons concerned thoroughly and ensure that they are complied with.

13.4 Control of the development or modification of the computer system

13.4.1 Request

(a) A request for the development or modification of the computer system must be made in writing, which may be an electronic transaction, such as e-mail, and approved by the competent authority, for example, the Head of the requesting Department or the person responsible for the information system.

(b) The impacts on important changes should be assessed in writing in terms of operation, security, and functionality of related work systems.

(c) The relevant government rules should be reviewed because the amendments in many cases may affect compliance with the said government rules.

13.4.2 Operations of system development

(a) It must have a separation of the computers for the work system development (Development Environment) from the computers for use (Production Environment) and access control to only those involved in each part. However, such separation may be divided by using different computers or by allocating space within the same computer.

(b) The requesters and external users should be involved in the development or modification process to develop the work system to meet the needs.

(c) It should be aware of the security and availability of the system from the beginning of development or modification.

13.4.3 Testing

(a) Requesters and the Technology Department as well as other relevant users must participate in testing to ensure that the computer system developed or modified has an efficient operation with complete and accurate processing and meets the requirements before transferring to actual use.

13.4.4 Transfer of the work systems for actual use

(a) The transfer of work systems must always be checked accurately and completely.

(b) There must be the preparation of documents and details to support the development of the work systems and the storage of the version of the developed work systems.

(c) There must be a collection of detailed information about the programs currently in use, which consists of details about past developments or changes.

(d) The documents supporting all work systems must be revised after the systems have been developed or modified to keep them up to date, such as supporting documents details of the data structure, the work system manuals, a list of authorized users, operating procedures of the programs, and program specifications, and such documents must be stored in a safe and convenient place for use.

(e) The program version must be kept before the development for use if the current version works incorrectly or cannot be used.

13.4.5 Post-Implementation Test

(a) After a period of use, the developed or modified systems should be tested to ensure efficiency of the operation, accuracy and completeness of the processing, and response to users' needs.

13.4.6 Communication of Changes

(a) Changes must be communicated to external users to use the work systems properly.

14. Use of information system services from IT Outsourcing

Objective

To protect the company's assets that are accessed by IT Outsourcing and to maintain a level of security and service as agreed in the service agreement.

Guidelines

14.1 The security requirements for the company's data must be established when there is a need for IT Outsourcing to access the data or assets in accordance with the requirements on data confidentiality of the company.

14.2 The data security requirements of the company must be communicated and enforced when it is necessary for IT Outsourcing to access the company's data or assets before granting an access.

14.3 In the Service Agreement, the outsourcing services shall be monitored, reviewed, and regularly evaluated.

14.4 If there is a change in the service agreement for critical systems, a security risk assessment must be carried out.

15. Information Security Incident Management

Objective

To provide a consistent and effective method for managing the information system security incidents, including notifying security incidents of the information system and weaknesses of the system security.

Guidelines

15.1 Duties and responsibilities as well as procedures must be established to deal with incidents related to the company's security.

15.2 Communication channels must be defined to clearly report security incidents of the information system.

15.3 If the user detects an incident which may affect the security of the information system, the user must report the incident to the Information Technology Department.

15.4 A security incident of the information system requires to be reported according to the severity of the incident. If it has a severe impact on a great number of users, it must be announced as soon as possible.

15.5 A breach of security must be recorded by considering at least the type of incident, quantity of incident occurred, and expenses incurred from damage to learn and prepare prevention.

15.6 Evidence must be collected and stored according to the rules or guidelines for reference in court proceedings.

16. Information Security Aspects of Business Continuity Management

Objective

To prevent disruptions in the company's operations due to a crisis or disaster and to prepare availability of the company's information system equipment.

Guidelines

16.1 The Information Technology Department must prepare a plan to solve problems arising from uncertainty and disaster that may occur with the information system according to the company's crisis management plan.

16.2 An inspection and assessment of potential IT risks must be conducted at least once a year.

16.3 The emergency preparedness plan must be reviewed at least once a year.

16.4 The availability of the backup information system must be checked at least once a year.

This Information Technology Security Policy was considered and approved by the Board of Directors at the Board of Directors' meeting No. 2/2025 on February 20, 2025. It shall be effective from February 20, 2025 onwards.

Note: This English translation is for reference purposes only. In the event of any discrepancy between the Thai Original Information Technology Security Policy and this English translation, the Thai original shall prevail.

....

Mr. Komol Rungruangyot

Chairman of Board of Directors

Euroasia Total Logistics Public Company Limited