noble

Noble Development Public Company Limited

Information Security Policy

TABLE OF CONTENTS

Information Security Policy

Noble Development Public Company Limited, hereinafter referred to as "the Company", is committed to providing Information technology systems, which is an important factor in running a standardized, modern, and secure business. It also aims to promote, develop the employee's knowledge and competency in the field of Information technology to enable them to work efficiently. Therefore, a policy on the use of Information technology systems has been established as a guideline for the operation of the executives and all employees.

Terms and Definitions

Terms used in this document

"Company"	means	Noble Development Public Company Limited and Continental City Company Limited.
"Authorized User"	means	Authorized User who has access to the usage, management, or maintenance of the Company's Information technology with their rights and duties depending on the following roles. **"Manager"** Director/equivalent to Director of Information Technology **"System Administrator"** Officers assigned by supervisors who are responsible for maintaining computer systems and networks that can access computer network programs to manage computer network databases. "**Employees"** employees, temporary employees, permanent employees, persons who are assigned duties by the Company or its employees.
"Data"	means	Text, news, documents, sound or anything else that can convey meaning in the form of numbers, languages, images, symbols unprocessed both in electronic form or in the form of printed materials and shall include computer data according to the law on offenses relating to computers and electronic data according to the law regarding electronic transactions.
"**Electronics Data**"	means	Data that have been created, sent, received, stored, or processed by electronic means, such as electronic data exchange methods. electronic mail, among others.
"Information"	means	Information that has been altered, processed, or analyzed, with the results summarized in different ways to convey the accurate intended meaning, or in a way which has practical value, to provide knowledge, understanding, analysis, decisions, and management strategy.
"**Third Party**"	means	Third parties, sellers, trading partners, vendors and contractors working for Noble Development Public Company Limited and Continental City Company Limited are allowed to have access and use Information

		System of Noble Development Public Company Limited and Continental City Company Limited according to their authority and responsibilities.
"**Information System**"	means	Information from Noble Development Public Company Limited and Continental City Company Limited, which uses computer and network technology to create Information, and can use Information to manage, plan, develop, control and support operations.
"**Network System**"	means	A group of computers and devices that are connected so that users on a network can communicate, exchange Information, and can use different devices in the network together
"**Standard**"	means	Norms applicable in actual operations to achieve an objective or goal
"Data Owner"	means	Persons authorized by superiors or positions to be responsible for the data of the work system where the owner of the data is responsible for that data or is directly affected if those data are lost.
"Property"	means	1. Information technology equipment and any other equipment that is used with all types of related Information technology equipment. 2. Instruction set, Information System program, and any other programs that are compatible with the program Information System. 3. Any Information and/or intellectual property.
"**Computer Equipment**"	means	Equipment or sets of equipment of a computer which connects via instructions or sets of instructions, other methods, and guidelines in using the equipment or sets of equipment for automated processing
"**Portable Equipment**"	means	Laptop, smartphone, or tablet which the Company authorizes to connect with the Company's Network System.
"**Software**"	means	Instructions, a set of instructions, or formats that are written, developed, or otherwise obtained for the purpose of collecting Information, deal with, and/or process the Information by electronic or other means which is applied to a computer in order for the computer to work or to have a particular effect, regardless of the nature of the computer language.
"**E-mail**"	means	A system that individuals use for sending messages to each other through computers and networks that are connected to each other. The Information sent can be text, photographs, graphics, animation and sound. The sender can send messages to one or more recipients.
"Password"	means	letters or characters or numbers that is used as a tool to verify the person's identity for the purpose of controlling access to Information and Information Systems and maintain the security of Information and Information technology systems.
"Malicious Software"	means	a set of instructions that damage, destroy, modify or add on to a computer, computer system, or other instructions, causing such computer or instructions to fails or does not work in accordance with the specified instructions.

"Storage Media"	means	Refers to electronic devices used to record or store data such as Hard drive or Flash drive or Handy drive or Thumb drive or External hard drive, etc.
"Breach of Security"	means	An event specifying the occurrence of a network service which indicates a likelihood of a breach of security policy, failed security, or an unknown event which may impose rick to security.
"Incidents Relating to Information Security"	means	Undesired or unexpected security incidents, which may cause the Company's System to be attacked, and security to be breached.
"**Social Network**"	means	Online social networking or a service that connects many people together through the internet. Examples of Social Networks include Facebook, Twitter, Blogger, etc.

Roles and Responsibilities

Information Technology Unit

(1) Set policies, plans, measures, methods, and audits related to the use and security of Information technology systems.

(2) Assess and manage the security risks of the company's Information technology system, emphasizing on the benefits and efficiency to the company, and delivers data along with practical principles to various business units.

(3) Keep track of computer threats both inside and outside the company

(4) Information Technology unit is in charge of designating accessibility, backup storage Information, and authorization that affects the business operations of the Company when such authorization is given by the responsible unit work systems or Information

(5) Determine common areas and access rights. Back up and maintain (Backup) data and users can access the system and access data only after approval from the data owner agency.

Data Owner and System Owner

Data Owner and System Owner are units who grant permissions of access to Users to the extent necessary to perform the Users' duty, as granting rights to access more than necessary will lead to unauthorized access. Thus, right to access must only be given based on the least necessary privilege.

Transferring Employees over Business Units / Resignation of Employees

In a case of employee transfer or resignation or no longer responsible for the usage of any computer system, such employee's unit must notify in advance, which shall include at least an effective date that such employee was to be not responsible for such computer system, the Information Technology unit to cancel his/her access to such computer system or change password in a case where such user id is still necessary.

Guidelines for Maintaining Information Security

Guidelines for maintaining Information security is developed in order to determine the criteria and methods for maintaining Information security in accordance with the policy guidelines set forth in Section 13 as follows:

Information security policies

(1) The Company must prepare a written Information security policy. Such policy must be approved by Board of Director and announce to be known by the Users.

(2) The Company must review and report consequences of the Information security policy at least once a year.

Organization of Information security

(1) The Company must designate the roles and responsibilities of the Users relating to the maintenance of security

(2) The Company must separate the duties and responsibilities of each unit apart from one another with the goal of minimizing the risk of unintended alteration to the data, unauthorized access, or usage of the Company's property in contrary to its purpose.

(3) The company must prepare a list of appropriate command lines or work approval lines, and notify such list to related persons

(4) The Company must prepare, update, and maintain a list of security experts to be up to date.

(5) The Company must specify Information security details in managing projects related to Information Systems.

Human resource security

(1) The Human Resource Management Department must examine and scrutinize the educational background, experience, and work history of Employees before accepting them as Employees.

(2) The Human Resource Management Department must scrutinize the qualifications of all applicants prior to accepting them as Management or Employee. They must not have a history of trespassing, altering, destroying, or stealing Information in the Information System of any organization.

(3) The Company has a signed operating agreement, including Information security agreements for Authorized Users.

(4) The Company must designate activities to support and promote awareness among Authorized Users in the Company's Information security system.

(5) The Company must conduct lectures, trainings, or develop Information security knowledge for System Administrators.

(6) On the termination of Employment, or upon a change on the nature of employment, the Authorized User must return properties relating to Information of their operation for the Company.

Asset management

(1) The Company must prepare a list of Information assets related to the Information System along with specifying the responsible person for asset transactions. The Company must ensure that such list is up to date.

(2) The Company must classify the type of data, confidentiality level, access rights, retention period, record of access, access channel, and retention location

(3) The Company must make a symbol or name plate on the data storage media to help control supervise data and Information, convenient to operate, and or conveniently released for further distribution.

(4) In the event that the User needs to remove the recording media out of the company, the User must register the borrowing in an inventory asset, and take care to prevent damage which occurs during the transmission of those recording media outside the Company and from unauthorized access.

(5) The Company must have appropriate and explicit methods for destroying data storage media. In the case where such destruction is done via a Third-Party service provider, a non-disclosure agreement shall be made.

(6) If the user brings an external portable computer to use and such usage cause damage to the Information System, the user is responsible for any damage caused. He must notify the Information technology department to resolve the issue.

Access control

(1) The Information Technology unit must establish access control procedures which must be regularly reviewed and updated.

(2) The Information Technology unit must establish a process for registration, update, and cancel user rights. This process must be kept as evidence for investigation if an issue arises.

(3) The Administrator must designate Information access rights as follows:

3.1) Root / High Privileged User.

3.2) Administrator.

3.3) User.

(4) The owner of the Information System must regularly review the access right at least once a year.

(5) Only administrators or authorized persons can modify the right to access the Information System

(6) Granting special privileges to users over normal use requires written permission from the owner of that Information System and specification of period of use. After the expiration of such period, the right shall be suspended immediately.

(7) The System owner must update the right to access of Users when employees resign, change position, or change duties.

(8) The system owner must manage the username account and Password responsible for that Information System, and must assign access rights to the system to users separately according to their responsibilities.

(9) Users must be made to cooperate with the Company's usage of Password (except systems with regulations) as follows:

9.1) Users must designate a Password with at least 8 letters.

9.2) Users must change the Password every 180 days.

9.3) Password shall at least be composed of three of the followings: capital letters, lower case letters, numbers, and special symbols.

9.4) Users shall not base their Passwords on names, surnames, and names of people who they are close to, or words from dictionaries.

9.5) Users shall not use automated Password recording systems

9.6) Users shall not disclose their Passwords to others or record their Passwords where it is easily accessed by other people.

9.7) Users should not allow others to use their username and Password for computer access

9.8) Users must insert their username and Password in accessing their computers, and should change their Passwords in accordance with the Company's use of Passwords.

(10) The Company must control access to Information System by the use of identity proofing using username and Password.

(11) Information Technology Unit shall control and limit access usage of program to only authorized Users.

(12) System administrator must control the access to the source code.

(13) Employees access to the system must be monitored and limited in accordance with roles and responsibilities.

Physical and environmental security

(1) Computer center area must be blocked with a wall and a door must be installed to prevent unauthorized access to Information.

(2) Electrical, communications, and other cables in the computer center area must be protected from unauthorized access, obstruction of the signal line or damage those signal cables.

(3) Computer center area must organize an area for access or delivery of products from Third Person to prevent unauthorized access to the Company's assets.

(4) The computer center area must have a proper security system against various threats that may occur with the equipment, such as installing fire-fighting equipment, closed-circuit television cameras, air conditioning system, and power backup system.

(5) Entering and leaving the computer central area must be authorized by the Company's administrators.

(6) The Information technology unit must specify the rights of users to enter and exit the computer center by requiring only relevant users to be able to enter-exit the computer center, such as administrators, etc.

(7) Users who want to access the computer center area must comply with the Company's computer center service guidelines. The Company must monitor the entry-exit of third parties and monitor the operation of third parties during their course of work within the Company.

Operations security

(1) The Information technology unit must plan the demand for additional Information resources in the future in order to make the system efficient and sufficient for practical use.

(2) The administrator must set time to computers within the Company using Network Time Protocol (NTP) to the server computer that provides time Information by setting the time of the host computer and the computer to the server computer that provides time Information.

(3) In case of change of equipment, Information systems, and network systems, the system administrator or developer must perform change management.

(4) If an administrator or an external service provider wants to use various tools for monitoring the network system or installing network equipment, such action must only be approved by the Company's management and installed by the Information technology unit.

(5) The Information technology unit must have a system for development and testing which is separated from the actual service system to mitigate the risk of unauthorized accessing or making changes to the system of the actual service.

(6) Users have the duty to install Software protecting the computer from malware and virus, including the duty to update such Software.

(7) If the user suspects that their computer has been attacked by malicious programs, Users are not allowed to connect the device to the company's network system in order to prevent unwanted instruction sets from spreading in the company's network system. The User should inform the Information technology unit for further action.

(8) The Information technology unit must conduct a review to update the version of the operating system and Software on the host computer to be up to date.

(9) Installation and connection to the host computer system must be performed by a system administrator

(10) The Information technology unit must require that there be logs of the Information system for the purpose of examining the use of the Information systems.

(11) The Company must store the Company's computer traffic data in compliance with the Computer Crimes Act B.E. 2550 and B.E. 2560, including the amended versions.

(12) The Company must arrange for access and modification of system rights details to be recorded for authorized and unauthorized people to be used as evidence in case where an issue arises.

Communications Security

(1) The Information Technology unit shall manage Network System into easily distinguishable zone, e.g., Network zone or Server zone, for the purpose of increase the ease of operation and the ability to control access to any equipment(s).

(2) The Information Technology shall install server or oversee the server installation.

(3) Network Systems which connect to other external Network Systems must do so through Firewall or Packet Filtering

(4) The Information Technology unit shall produce and make up to date Network diagram, which shall at least contain details of internal network(s), external network(s), any network equipment, and data classification.

(5) Network administrator must regularly verify user's right to access Network System.

(6) System administrator must prescribe minimum quality of security and service level for external Network service which the Company may use.

(7) The Information Technology unit shall prescribe and annually review Network's SLA.

(8) Users are forbidden to disclose IP Address, Network diagram, Configurations, or any information relating to network and information system connected to an unauthorized person or third party.

(9) System administrator shall provide the system with appropriate security measures capable of information exchange between companies or Third Parties.

(10) Users shall not connect to the internet through the smartphone while connecting to the Company's Network System.

(11) Users are forbidden to broadcast or signal wireless Network Systems to another person while connecting to the Company's Network System.

(12) The network service agreement shall prescribe quality of service provider e.g., must be knowledgeable in network management or possess a certain certificate(s).

(13) The network service agreement shall prescribe the quality of service's security to ensure security in providing network service e.g., identification, encryption, network connection.

(14) The network service agreement should allow the Company to audit service provider.

System acquisition, development and maintenance

(1) The development, acquisition, and maintenance shall be authorized by person in authority prior to such development, acquisition. Or maintenance.

(2) The Company shall prescribe Secure development policy and enforce such policy in internal development.

(3) System development shall adhere to the following principles;

3.1) Least Privileges,

3.2) Need to know,

3.3) Defense in-Depth,

3.4) Open Design, and

3.5) Security Engineering Principles.

(4) System development shall be conduct under the following security policies;

4.1) Confidentiality,

4.2) Integrity,

4.3) Availability,

4.4) Identification,

4.5) Authentication,

4.6) Authorization,

4.7) Audit Logging,

4.8) Mandatory security measures e.g., OWASP Top 10, SANS Top 20, etc., and

4.9) Continuity.

(5) Developer may develop any program or hardware, but shall not;

5.1) Develop program or hardware in a way that damage system security mechanism, including unauthorized usage of password, making copy of data of another person, or decryption of password of another person,

5.2) Develop program or hardware in a way that grant user more right and priority to system resource than other users.

5.3) Develop program which shall duplicate or embedded with other program in a manner similar to worm or malware.

5.4) Develop program or hardware in a way that damage license access control software.

5.5) Exhibit illegal data, Piracy, exhibit inappropriate message and picture or message and picture which go against good morals and traditions of Thailand in any communication channel.

(6) Software development shall be conducted in accordance with web-application development standard

(7) Changes to system in development cycle e.g., SDLC procedure, shall be controlled by official changes control procedure

(8) Changes to environment relating to application shall be test to ensure non-impact on the Company's business continuity or information security prior to official launch.

(9) Changes to software package shall be prevent necessary change and all change shall be strictly controlled.

(10) The Company shall prescribe and maintain environment's security for appropriate development

(11) Outsourcing software development shall be verified and monitored by system owner and the Information Technology unit

(12) System development shall be subjected to security function tests during the development

(13) There shall be tests and criteria for examining new information system. If improvement is necessary, the system shall be appropriately updated.

(14) There shall be test data control. Real data in an actual working system should not be used for the test. In a case where real data are necessary for testing, the data should be replaced or marked in a way that cannot be traced back to real data.

Supplier relationships

(1) System owner are responsible for granting access to information system. The Supplier shall put in writing the request to access, which shall contain at least the following;

1.1) Purpose of accessing the information system,

1.2) Term of access, and

1.3) System owner's consent to take responsibility for bringing Third Party into and operating in the Company.

(2) The company, which is the partner of the contract, working for the Company, whether on-premise or not, shall sign the contract. The contract shall be signed prior to granting access to such Third Party into the information system.

(3) The company, which is the partner of the contract, developing information system shall sign a non-disclosure agreement and summarize information security details for the Supplier.

(4) The Company shall ensure that the Third Party diligently maintains security, including confidentiality, integrity, and availability.

(5) The Company shall monitor and ensure that the operation of the Supplier is in accordance with the agreed-upon scope.

(6) In an event of changes in term of service and/or service format or technology, stakeholders, together with the Supplier, shall review and revise the contract.

(7) Upon detecting Breach of Security, the Supplier is required to immediately notifying system owner of Breach of Security. The system owner shall notify the Information Technology unit and system administrator of such a breach.

Information security incident management

(1) The Company shall prescribe roles and procedures for Information security incident management to ensure an organized, prompt and effective response to information security incidents.
(2) The Company shall provide a proper and swift channel for information security incident reports.
(3) System owner shall analyze and solve unexpected or undesirable information security incidents.

Information security aspects of business continuity management

(1) The Company shall develop and make up to date business continuity-ensuring plan, including plan test run at least once every year.
(2) The Company shall prepare backup information processing equipment and computer center in accordance with the prescribed availability requirements.
(3) Users shall adequately backup data relating to operation to ensure business continuity in an emergency.

Compliance

(1) The Company shall regularly, or in and event of significant changes, review information security management.
(2) Users must take precautions to not use unlicensed software. The Company is not responsible for any liability arising from users' usage of unlicensed software.
(3) The Company shall conduct a security risk assessment at least once every year.
(4) The Company shall put in place an assessment method and assess information security. The assessment shall be carried out by internal audit or external audit.

Users' information system regulation

Users of the Company information system are responsible for following the Company's Information Security Policy and this regulation as follows.

Usage of information property

(1) Users may hold computer equipment, Notebook, or PC / All in one PC for the purpose of the Company business.
(2) Users are responsible for taking care of and are liable for damage or loss of information property and/or information equipment in which the Company entrust to users and allowed users to used such property and/or equipment as users' own property.
(3) Users are responsible for compensating the Company of damages arising from damage or loss of information property and/or information technology equipment in which the Company entrust to users in accordance with the property's value or actual damages if the cause of damages is as follows;
    3.1) Users' intention or negligence,

3.2) Misuse or usage outside of the Company's business, and

3.3) Allowing other person, whether he/she is the Company's personnel or not, to use computer equipment. Except in a case of written document, approve by C-level, allowing other person, who is not the holder, use computer equipment.

(4) Users shall only utilize information property and/or information technology equipment, which are prepared by the Company, in the Company's business. Users are forbidden from utilizing such property and/or equipment outside of the Company's business, or installing software or hardware or the purpose outside of the Company's business in any case, whether such installation shall cause damage to such property and/or equipment or not.

(5) Users holding computer equipment, Notebook, or PC / All in one PC may only use computer program which the Information Technology unit installed. Users are not permitted to install and program on the computer. Detection of piracy for the purpose of installation and usage on such computer constitutes a breach of the Company's Information Security Policy, even if it was for the purpose of the Company business, and Users shall be solely responsible for any damage arising from such piracy.

(6) In a case where users wish to install a program, that the Information Technology unit did not provide, for the purpose of work in the Company business, users shall make a request to install such program to the Information Technology unit. If the Information Technology unit's examination of such a program indicates that such program may cause harm to the Company's information system, the Information Technology unit hall cancel the request.

(7) The program provided by the Information Technology unit is considered necessary to work. Users are forbidden from deleting, altering, editing, or making copies to use for other work. Except allowed by a C-level or person assigned with a respective software license.

(8) Data within the computer are considered confidential and property of the Company and must be stored within the assigned area. It is forbidden to make copies or duplicate such data to other persons or Third Parties. Except in a case of a written consenting document, approved by C-level.

(9) Users shall not leave important documents or storage media unsupervised or unused and shall safely store such document or storage media safely e.g., in a locked cabinet.

(10) Users shall not leave important documents on the photocopier, printer, or scanner. Users shall collect such documents immediately after putting in the printing order.

(11) In a case where data become no longer necessary, users shall dispose of such data within storage media. Users shall verify the category of data within storage media and sort out storage media in accordance with category or data class and dispose of such data in accordance with the Company's disposal method of the respective data class.

(12) Users are forbidden from saving not copyrighted file e.g., music, picture, video, movie, within the Company's computer equipment, Notebook PC / All in one PC. The Information Technology unit shall dispose of such file immediately upon detection.

(13) Users are forbidden from reusing documents containing important data.

13.1) To prevent attack or threat on the Company's Network System from outside, users are forbidden from connecting computer with other Network System while connecting with the Company's Network System.

13.2) Users are forbidden from stalling or activate wireless network equipment within the unit, whether Access point, Wireless Router, Wireless USB Client, or Wireless Card without the Information Technology unit's consent.

13.3) Users shall dispose of important data on paper or temporary material e.g., CD/DVD, after it is no longer necessary for work by ensuring it becomes unreadable and cannot be reused.

13.4) Users shall return information property and/or information technology equipment to the Company immediately after it is no longer necessary for work or when the employment is terminated or when the Company asks for it back.

Access and usage of information system

(1) Users who need to use the Company's information system and work system shall ask for approval from person who is authorized to give approval for the Information Technology unit to grant the access.

(2) Users are forbidden from the followings

2.1) Know user id and password of other, including using other's user id and password, and

2.2) Allowing other to use, disclose, distribute, or make other became aware of his/her own user id and password.

(3) Users shall protect and take care of his/her own user id and password information. If users became aware that his/her user id and/or password information are disclosed, he/she must change their password immediately.

(4) Users shall always identify him/herself prior to accessing the Company's information system or work system. If users cannot successfully identify him/herself e.g., forgot password, the password is locked, or other mistake or error, users shall notify the Information Technology unit immediately.

(5) Users shall lock the computer screen when it is not in use and shall be required to identify him/herself again upon resuming the usage of the computer.

(6) Users shall log out from the work system at E.O.D. or when it is no longer necessary for work.

(7) The Company's personnel are forbidden from playing unlicensed music and music which the Company did not put into the Company's broadcasting system, including playing music from copyrighted gramophone records or from public networks e.g., YouTube. As such act will violate Copyright Act B.E. 2537 for broadcasting works to the public without the copyright owner's consent.

(8) Immediately report any defect or error to the unit director and Information Technology unit for repair upon detecting abnormality, defectivity, or any hindrance to work on the information system or work system.

(9) Users, who detect Breach of Security or weak point in the Company's system shall not inform any person except supervisor and Information Technology unit. Users are forbidden from proving any suspicion on security weak spot by him/herself.

(10) Users shall be responsible for any action within the Company's information system in his/her user id, whether such action is users' action or not.

Usage of E-mail

Information Technology unit has provided the Company's personnel with personal E-mail for the purposes of work in the Company's business. Personnel shall take precautions in using E-mail and follow the following regulations.

(1) When users are assigned a user id for the E-mail system, users shall log in with the given user name and password and shall immediately change the given password into a new password.

(2) Users shall not use other E-mail system user id to read, receive, or send a message, except if the user id owner consent and that user id owner shall be responsible for the usage of his/her own E-mail.

(3) To prevent sending an E-mail to the wrong receiver, users shall always verify the E-mail receiver address before sending any E-mail.

(4) Users may provide details information within E-mail Signature, including name, position, unit, company name, phone number, and E-mail user id.

(5) It is forbidden to use the Company's E-mail for the followings;

5.1) Sending Spam Mail,

5.2) Sending Chain Letter,

5.3) Intentionally sending mail containing virus(es) to another person,

5.4) Use indecent language, or send or receive inappropriate E-mails which may damage the organization's reputation or cause division between organizations through E-mail.

5.5) Receive or send E-mail containing illegal, hateful, pornography, harmful intention, threatening, hurtful, deceitful, libel, slander or hateful, or supporting criminal acts or disturb peace or morals or violate the Company's policies.

5.6) Use the Company's E-mail for advertisement or for the benefit of him/herself or another person who is not related to the Company's business.

5.7) Sending the Company's E-mail together with external E-mail.

5.8) Disclose the Company's Email Account to another person in any way e.g., post on a web board, or questionnaire from a partner, except for the benefit of the Company or approved by a person with approval power.

5.9) Send a message containing personal opinion but claim to be the Company's opinion or causing damage to the Company.

(6) Users shall verify the attached document for viruses by anti-virus program from E-mail before opening any documents to prevent opening any processable file.

(7) Users should manage his/her data file and E-mail to keep only the necessary file and E-mails and should delete unwanted E-mails from the system to reduce the usage of the E-mail system's space.

(8) To prevent the breach of the Company's confidential information, users are forbidden from using E-mail outside of the Company's Network System e.g., Hotmail, and Gmail, for sending the Company's important data.

(9) Users are forbidden to use any electronic means to wrongfully trap computer information of another person between sending in computer systems, whether it is picture, sound, or any other things within Network System information of the Company or Third Party.

Internet usage

(1) Users shall always keep in mind of security of information sent or received through the internet.

(2) Users shall not download open or use instruction sets, work system programs, or data on the internet network in a way that may be considered piracy, or endanger the Company's security.

(3) Users are forbidden from downloading files or pictures that;

3.1) May violate Computer Crime Act B.E. 2550 and B.E. 2560 as amended,

3.2) May violate Copyright Act B.E. 2537 as amended,

3.3) Containing virus or Malicious Code, and

3.4) Not related to the Company's business.

(4) Users shall not use services on the internet which use a large quantity of Bandwidth or over a long period of time during working hours e.g., do not open or use entertaining online programs, do not open or use Peer-to-Peer programs, or programs presenting the same level of risk such as Bit torrent.

(5) All Personnel shall keep in mind of the security in using Social Networks e.g., disclosing the Company's secrets which may negatively affect the Company's image.

Working from outside of the office

(1) Users who wish to access the Company's internal network by Remote Login shall request approval from a person with approval power before accessing such network.

(2) In a case where users need to take portable communication equipment, which is the unit's public information property, users shall put a request to take such equipment to the supervisor and Information Technology unit. Users shall immediately return such equipment when it is no longer necessary for work.

(3) Users who need to take the portable computer outside of the office shall use such computer with precaution, shall not leave such computer in public with no supervision, and shall not allow another person to use such computer to prevent unauthorized access or disclosure of information.

(4) Users shall, at all times, take precautions to not lose the portable computer and lose the information within such computer.

(5) Users shall not connect the portable computer to unknown Public Wi-Fi.

(6) In a case where users need to work from outside of the office and need to connect to the Company's system, users shall connect through the channel provided by the Information Technology unit.

Work system, news, and information management

(1) Users are responsible for preventing and look after instruction set, work system program, property, and information of the Company. In a case of loss, damages, wrongful usage, unauthorized disclosure, whether intentionally or through negligence, users shall be liable for the damages.

(2) Users are responsible for utilizing the instruction set, program, working system, property, and information of the Company, which the Company has provided, only for the purpose of the Company's business.

(3) Instruction set, work system program, property, and information which users develop or create for the purpose of the Company's business copyrights and ownership solely belong to the Company.

(4) Users are forbidden from utilizing the Company's information system as follows;

4.1) Brining the following information into the Company's information system or Third Party's system

- Fake information, whether partly or in whole, or false information, in a way that may cause damage to the Company, Third Party, or the customer,
- False information in a way that may ruin the country's stability or cause the people to panic,
- Any information which is considered a crime to the stability of the kingdom or a crime relating to terrorism, pursuant to the Criminal Code,
- Any information which is considered hateful, pornography, harmful intention, threatening, hurtful, deceitful, libel, slander, or hateful and can be accessed by the people.

4.2) Knowingly spread or forward the above-mentioned information 4.1)

(5) It is forbidden to bring information about other person's pictures into the Company's information system or Third Party's system which the people may access. If such a picture is created, edited, added, or altered by electronics or any other means, in a way that may cause such a person to be disreputable, looked down upon, hated, or disgraceful. Except where it was done in good faith.

(6) Do or refrain from, which is considered or may be considered as punishable according to Computer Crime Act, laws, or any regulation to which the Company must comply.

Compliance with the laws and regulations

(1) To prevent damages and enable the Company business to be able to effectively proceed, users shall act in accordance with the policies, regulations, and rules of the Company, including information technology laws, to which the Company must comply.

(2) In a case where users violate the Company's policies, regulations, and rules, including any laws, to which to Company must comply, it is considered a personal offense in which the user shall be punished pursuant to the Company's policy and if such act violates Computer Crime Act, or Copyright Act, or any other related laws, he/she may be persecuted.

Effective 22nd February 2023

(Mr. Thongchai Busrapan)
Co-Chief Executive Officer
Noble Development Public Company Limited