Global Power Synergy Public Company Limited's

Regulations on Information and Communication Technology Policy Standard Practice

2021

To ensure that GPSC and its affiliates' Information and Communication Technology (ICT) governance, direction, and management will be clearly implemented and understood in the best practices which lead to appropriate implementation, information security, continued support towards GPSC and its affiliates' operations, protection of confidential corporate and personal information, and compliance with relevant laws of the Kingdom of Thailand, the Information and Communication Technology System Policy and relevant practices are announced in the details mentioned below.

Section 1

General Provision

1. The following documents are to be canceled:

1. 1 Global Power Synergy Public Company Limited's Regulations on Information Technology Security Management 2014

1.2 Global Power Synergy Public Company Limited's Announcement No. 014/57, Re: Good Information and Communication Technology Governance

1. 3 Global Power Synergy Public Company Limited's Announcement No. 015 /57, Re: Information System's Environmental Friendliness Policy

1. 4 Global Power Synergy Public Company Limited's Announcement No. 016 /57, Re: Personal Information Protection Policy

1.5 Global Power Synergy Public Company Limited's Regulations on Information and Communication Technology Policy Standard Practice 2017

1.6 Global Power Synergy Public Company Limited's Regulations on Information and Communication Technology Policy Standard Practice 2020

2. Scope

This provision covers the management, protection, and security of the Company's information and cyber system, both inside and outside its establishments, and the cloud service procured by the Company. This provision would be enforced against the following people:

2.1 All managements, employees, and divisions of GPSC;

2.2 External personnel authorized to access the Company's computer and information system properties or resources; and

2.3 Affiliates of which GPSC possesses the power to control Management and provide Information and Communication Technology systems.

3. Terms and Definitions

- "GPSC" or "Company" means Global Power Synergy Public Company Limited.
- "Chief Executive Officer" means the President and Chief Executive Officer of Global Power Synergy Public Company Limited.
- "Regulation" means Global Power Synergy Public Company Limited's Regulations on Information and Communication Technology Policy Standard Practice 2021.
- "Employee" means any employees of GPSC and its affiliates as well as the personnel who are hired by the Company.
- "User" means the Company's employee or the external personnel who are authorized to use, manage, or maintain its information system. The user would own an account and password to access the Company's information system and/or information processing tool.
- "Executive" means GPSC's authorized high-level personnel who hold a position of at least senior vice president.
- "Supervisor" means an authorized person according to the organizational structure.
- "System Administrator" means a person who is assigned by the Supervisor to maintain the computer system and network. The system administrator can access the computer system program in order to manage the network database.
- "System Owner" means a unit of GPSC which takes responsibility for owns the information system and/or information technology systems that operate in the system according on the duties and responsibilities.
- "Information Responsible Unit" means a unit of GPSC which takes responsibility for the information systems that operate in the system according on the duties and responsibilities.
- "Contractor" means a juristic person or its representative who works for GPSC through an engagement done in accordance with the Company's procedure within a period specified in the contract.
- "Intern" means a student who is allowed by their university or educational institute to take an internship with the Company within a period specified in the agreement between the Company and the institute.

- "Information Operation Controller" means a person who is assigned to control and manage the information, information system, and network system of GPSC.
- "System Developer" means a person who is assigned to develop or improve GPSC's operation or support systems for tasks done via the information system.
- "User's Rights" mean general rights, specific rights, special rights, or other rights relevant to the Information and Communication Technology system of GPSC.
- "Computer service unit" means a unit which takes responsibility for GPSC's information technology system management.
- "Computer" means a tool that processes data/information through an operating system. This tool is inclusive of a processor, monitor, and keyboard.
- "Mobile Device" means a device that can be carried easily. This device works with an operating system. It can receive an input, display an output on the screen, and access Wi-Fi network. Examples of mobile devices include smartphones, phablets, tablets, netbooks, notebooks, etc.
- "Network Equipment" means a equipment or a set of equipment connected with a computer or the computer network in order to exchange data/information or share resources.
- "Computer Network" means a network in which computers, computer tools, and computer data are connected to provide shared resources.
- "Computer Data" means data, text, instructions, software, or other elements in a computer system which can be processed by the computer system. This may include electronic data determined by the Electronic Transactions Act.
- "Information System" means the processing done by computer or electronic tool in order to create, receive, send, store, display or process electronic data. This also includes devices that serve the Company's information operations. However, the information system which controls machinery and manufacturing tools is not included.
- "Social Network" means a system which enables communication, news acknowledgment, and information sharing with an enormous amount of people on the internet via social media.

- "Property" means the information, information system, and Information and Communication Technology properties of GPSC, such as GPSC's computers, mobile devices, social network, or the software of which copyright is reserved by GPSC.

- "Third Party" means an external organization which GPSC authorizes to access and use the Company's information or properties. The third party shall be authorized for access according to their responsibility and shall maintain confidentiality of the information.

- "Information" means a fact obtained from processing or management of numeral, text, or graphic data into an easily understandable form which can be used for management, planning, decision making, and other operations.

- "Computer System" means the computer or set of computers of which operations are connected by instruction, software, or others. This also includes procedures implemented to set the device or set of devices to automatically process data.

- "Network System" means the network used for communication and exchange of data and information between different technology systems used in the organization, including LAN, intranet, and internet.

- "LAN" means electronic network systems which connect the organization's computers together in order to exchange information within the organization.

- "Internet" means an electronic network system which connects the organization's computer networks with the international internet.

- "Information Technology System" means the organization's operation system where information technology, computer systems, and network systems are used for creating the information which can be used for planning, management, service support, and communication development and control. This system consists of computer systems, network systems, programs, data, information, etc.

- "Information and Communication Technology System Workspace" means a space where the organization allows Information and Communication Technology usage. The workspace includes the following spaces:

- "General Working Area" means a space where a personal computer or notebook is installed at the workstation.

- "Information Owner or Information System Owner" means a person who is assigned by the commander to take responsibility for an information or work system. The responsible information owner shall be directly accountable if information loss occurs.

- "E-mail" means a system where persons can send and receive messages via a computer and connecting network. The data the can be sent includes text, photos, graphics, moving pictures, and audio. The sender can send messages to one or various recipients. The standard mail protocols include SMTP, POP3, and IMAP.

- "Password" means the letters, alphabets, or numerals used as an authentication tool in order to control information and system access for the security of such information and technology system.

- "Malicious Software" means software which causes a computer, computer network, or other software to be damaged, destroyed, modified, malfunctioned, or in error.

- "External Personnel" means the external persons or organizations operating businesses or services who are authorized to access the Company's information and information processing tools. External personnel include business partners, outsourcers, suppliers, service providers, and consultants.

- "Essential Information" or "Sensitive Information" is the information which is essential to business operations or the information which the Company is liable for as required by law, business ethics, or contract stating that the Company shall not disclose such information to third parties or utilize it for any other purposes than the purpose of business operations. Leakage of essential or sensitive information may cause the business operation to be halted and ineffective, or may cause a negative reputation.

4. Security Principles

4.1 These security principles aim to achieve the following purposes:

4.1.1 Confidentiality: to protect information confidentiality by preventing information, including personal information and other information owned by the Company, access and disclosure by unauthorized persons;

4.1.2 Integrity: to ensure that the Company's information would not be revised, modified, or destroyed by unauthorized persons;

4.1.3 Availability: to ensure that authorized users can instantly access information and service with trust;

4.1.4 Accountability: to determine the role and responsibility of each person and assign accountability towards the results of such role and responsibility;

4.1.5 Authentication: to ensure that computer and information system access rights shall be given only after complete authentication;

4.1.6 Authorization: to ensure that authorization for computer and information system access is done with least privilege and is in compliance with the need to know basis as allowed; and

4.1.7 Non-repudiation: to ensure the parties who are involved in the operations shall be unable to repudiate their involvement in such operations.

4.2 To achieve effective security, mutual agreement and serious attention are required for all relevant aspects, including:

4.2.1 All employees and relevant external personnel shall be responsible for security.

4.2.2 Security management and operations shall be continuously done.

4.2.3 Consciousness and awareness of one's own duty and responsibility to comply with the practices detailed in policies, standards, frameworks, procedures, instructions, and processes are the most vital elements for security operations. To achieve effective security, all employees and external personnel shall be provided with an explanation to clearly understand their own duty and responsibility in the security operation they are involved in.

5. Enforcement and Exemption

The implementation of this policy will be monitored and inspected by the Company's management. The enforcement conditions shall be the same as other rules and regulations of the Company.

GPSC employees of all levels who do not comply with this policy shall be subjected to disciplinary action and may be subjected to criminal and civil prosecution. The relevant third parties who fail to comply with this policy shall be reported to the relevant management or executives of the Company for them to inspect and execute contract revocation or other legal measures.

The request for compliance exemption shall be done in written form and in accordance with the compliance exemption request procedure applied for other policies.

6. Review and Revision

This policy shall be reviewed and revised by the Company's information technology department at least annually in order to maintain its consistency with business needs and relevant laws.

Section 2

Information Security Policy

1. Purpose

To ensure that GPSC and its affiliates' Information and Communication Technology (ICT) operations are done appropriately, effectively, and in compliance with international standards, while the information security aspect is covered and any issues that may be caused by information technology misuse and threats are prevented, information security management is determined as detailed below.

1.1 Establish a security management policy for information and communication technology and other relevant policies. To comply with various of IT-laws that the Company should follow in order to create confidentiality and security in Information and Communication Technology system or the GPSC's computer network to effectively and efficiently operate.

1.2 The scope of Information and Communication Technology security management shall be identified accord to ISO/IEC 27001 or similar standards, and frequently revised.

1.3 Regulations on information security shall be established in order to set guidelines and instructions for appropriate operations.

1.4 While working, the management, employees, system administrators, and external personnel who work for GPSC shall be aware of the importance of information security and shall strictly adhere to the relevant policies and regulations.

1.5 Information security risk assessments and management shall be done in order to prevent threats which may affect the Company's business operations and review at least once a year.

1.6 Analysis of situations, which may cause information system damage, loss, or information leakage, shall be done in order to set up corrective and preventive measures.

2. Policy

The information technology security management policy consists of various vital topics as mentioned.

Topic 1

Information Technology Risk Assessment

1. Information technology risk assessments shall be supported to be performed in all relevant aspects in accordance with the policy or guideline determined by the risk division.

2. Improvement processes shall be established in order to eliminate the existing risks and minimize risks until they are at the level that can be accepted by the Company.

3. Risks shall be frequently reviewed and improved in compliance with the current circumstances.

Topic 2

Segregation of Duties

1. The information technology division structure shall be established with explicit duties and authorities. There shall be job descriptions which identify the duties and responsibilities of each position. For example, the personnel who work as developers and those who work as system administrators shall be separated.

2. Duties and responsibilities of the personnel who are relevant to this regulation shall be determined by the guidelines mentioned below.

2.1 Duties of the Chief Executive Officer

2.1.1 Determine overall strategy as well as support, suggest, and approve the policies and regulations on the information and communication system.

2.2 Duties of the Management and Executives

2.2.1 Encourage, support, suggest, or cooperate in the approval of information and communication system related processes and documents.

2.3 Duties of the GPSC GROUP Digital Platforms Division Manager

2.3.1 Assess information resource needs and values as well as procure and improve the information system in accordance with the Company's strategy.

2.3.2 Manage the Company's information resources to be able to effectively support internal operations.

2.3.3 Determine targets and establish regulations, policies, procedures, and measures relevant to information system security and usage in order to achieve confidentiality, integrity, and availability.

2.3.4 Manage the monitoring of various attacks which may be done against the information system. Determine responsive measures and encourage business operation continuity in order to recover the system after attacks occur.

2.3.5 Manage and analyze risks which may halt the information system resulting in negative effects to business operations.

2.3.6 Present security or significant information and progress of work relevant to the information system to executives according to the occasion and as appropriate.

2.4 Duties of the Users

2.4.1 Keep updated, understand, and strictly adhere to the enforced regulations, policies, procedures, and measures on information system security and usage.

2.4.2 Be fully cooperative in the usage, sending and receipt of information, and information distribution in order to secure the safety of the system, and comply with laws and corporate regulations.

2.4.3 Immediately report to the information division if there is any situation that may cause risk or damage to the system or the information.

2.5 Duties of the System Owners or Information Responsible Unit

2.5.1 Create an access control document and establish the information access control measures and procedures in accordance with regulations or policies on information system security and usage.

2.5.2 Maintain the information and system. Control and approve access to the information or the information system in own's or division responsibility. Also, frequently review the access rights to ensure correctness and appropriateness.

2.5.3 Inform the information technology division to give, revoke, or make changes to the access rights when a user's duty is changed. Also, immediately report any situation that may cause risk or damage to the system or the information.

2.6 Duties of Internal Audit

2.6.1 Conduct audits on information system security and usage related managements, operations, and activities as appropriate and required.

2.7 Duties of the authorities of Information responsible unit

2.7.1 Keep updated, understand, and strictly adhere to the enforced regulations, policies, procedures, and measures on information system security and usage.

2.7.2 Create an access control document and establish the information access control measures and procedures in accordance with regulations or policies on information system security and usage.

2.7.3 Immediately report to the direct commander in the information technology division if there is any situation that may cause risk or damage to the Company's system or information.

2.7.4 Encourage and help the users to understand the regulations, policies, procedures and measures on information system security and usage. Also, encourage the compliance of activities with such regulations, policies, procedures, and measures.

Topic 3

Human Resource Security

1. The system owners shall define duties and responsibilities of the external personnel or the third parties hired by the Company on information system security shall be determined in the written form and complying with the Company's information system security policy.

2. The system owners shall establish the vendor and the organization shall mutually sign a non-disclosure agreement (NDA) which is one of the documents required for an engagement. This agreement shall have binding force during the engagement period and for at least 1 year after the engagement period is over.

3. In order to correctly manage user accounts and keep them up to date, the human resource department or the relevant departments shall immediately report to the information technology division regarding the following issues:

- employment/ engagement
- change of employment/ engagement condition
- retirement or withdrawal from the status of being the Board Committee or the Company's employee
- position transfer

4. The Information responsible unit shall inform the external users and organizations hired shall acknowledge the currently enforced regulations or policies on the Information and Communication Technology system.

5. The new employees shall be trained about the currently enforced regulations or policies on the Information and Communication Technology system.

6. If there is any change, the engagement is revoked, or the end of project is reached, access to all information in the system shall be revoked.

Topic 4

IT Resource Management

1. IT resources, such as databases, files, software, development devices, computers, network tools, communication devices, external hard drives, and all types of connectors, shall be listed in the records in order to be systemically controlled by the GPSC Group Digital Platforms Division and/or Information Responsible Unit. Also, the labels attached on documents and IT resources for clear identification shall be appropriately defined.

2. The GPSC Group Digital Platforms Division and/or Information Responsible Unit shall establish a procedure of Data created, stored, or sent via the Company's information system shall be deemed to be the Company's property. They shall be managed and controlled to be accurate and secure. However, the data, software, or other resources owned or licensed by the customer or third party or protected by patents shall be excluded.

3. The Information Responsible Unit shall establish preventive measures and information management procedures in accordance with the information confidentiality and importance level determined by the Company. This aims to secure the safety of IT resources with appropriate methods. Documents or printed material which are reissued or copied, fully or partly, from a master copy that is identified with confidentiality levels shall be deemed to be identified with the same confidentiality level.

4. The Information Responsible Unit shall establish an appropriate procedures or guidelines on resource usage in written form in order to prevent IT resource damage.

Topic 5

Access Control Security

1. Access and Usage Control Procedure

1.1 Entry and exit of the site where an important IT system is installed shall be strictly controlled. Only the authorized persons can enter such sites when necessary.

1.2 The division manager of Information Responsible Unit or the employee assigned by such manager of Information Responsible Unit shall be authorized to approve or revoke IT system access rights.

1.3 Only IT system administrators or authorized persons can determine or change information and system access rights in order to make them consistent with the user's usage manner and responsibilities, and revoke access rights when the user retires or transfers to different position. Also, such personnel shall review the access rights at least once a year.

1.4 Important incident and IT system usage record systems shall be established together with an appropriate procedure on the important information system safety verification or assessment.

1.5 Approval result and rights revision request procedures shall be determined in order to allow systematic control. The record of such activity shall be done for future inspection.

1.6 The assigned access rights shall allow the user to access only information necessary for their work in order to prevent excessive usage. Therefore, the system administrator or the authorized person shall assign access rights only to the minimum extent necessary.

2. User Authentication

2.1 A user authentication system or process shall be put in place in order to verify the user's identity before every login. The user shall remember and store the password or authentication data as personal confidential data and shall not disclose such data to others without an appropriate reason.

3. Access Management in Accordance with Confidentiality Level

3.1 The Information Responsible Unit shall determine access, management, maintenance, and destruction procedures in accordance with the type and confidentiality level assigned to such information by the Company.

4. Network Access Management

4.1 Responsible personnel shall be authorized according to duties and responsibilities. Approval result, rights revision, and parameter change request procedures shall be determined in order to allow systematic control. The record of such activity shall be done for future inspection and the parameter determination review shall be done at least once a year.

4.2 Network systems shall be designed separately according to different types of IT services used by the user or groups of IT systems, such as internal zones, external zones, and VLAN segmentation. This is to allow systematic control and prevention of intrusion, and to restrict the user to access only the allowed network.

4.3 All connections of the Company's network with other networks, such as Plant Information's network (PI network) or external networks, shall be done via an intrusion prevention system, such as a firewall, which is a minimum prevention measure.

4.4 Installation and connection of devices, connection between networks, or changes in network shall be approved by the GPSC Group Digital Platforms division manager or an authorized person before any execution.

4.5 Procedures on control, monitoring, and prevention of system intrusion shall be established. Also, recovery and responsive measures for network intrusion or damage shall be put in place.

5. Server Management

5.1 Responsible personnel shall be authorized according to duties and responsibilities. Approval result, rights revision, and parameter change request procedures shall be determined in order to allow systematic control. The record of such activity shall be done for future inspection and the parameter determination review shall be done at least once a year.

5.2 The server or virtual server shall be equipped with intrusion prevention system, such as endpoint protection and firewalls which are minimum prevention measures and shall be provided only as necessary. If the necessary service encounters any risk against the security system, an additional preventive measure shall be put in place.

5.3 All software shall be updated and kept up to date in order to frequently fix loopholes in the system software. If updates cannot be done, programs in the server may encounter risks against the security system and an additional preventive measure shall be put in place.

5.4 Installation and connection of servers shall always be approved by the GPSC Group Digital Platforms division manager or the authorized person before any execution and shall be done only by IT personnel.

6. Record and Inspection Manager

6.1 System logs, application logs, and records of intrusion prevention system, such as end point protection and firewall, shall be done as appropriate in order for these logs and records to be analyzed for intrusion prevention improvement.

6.2 Log revision preventive measures shall be put in place and the access rights shall be limited only for relevant personnel or analysis systems. The distribution of logs to external service providers shall be done only after approval by the GPSC Group Digital Platforms division manager or authorized personnel.

7. Remote Access

7.1 A process or method of remote access shall be determined. The authentication and port used for system login shall be strictly controlled. Also, the remote access shall be done only as necessary. All the execution shall be done only after approval by the GPSC Group Digital Platforms division manager or authorized personnel.

8. Access Control to program Source Codes

8.1 The Information Responsible Unit shall define the access control to program Source Codes only necessary for pertinent user's purposes, as well as update the user's right list to keep current the user and access right data.

8.2 The Information Responsible Unit responsible for storing Source Codes shall provide logging records which show the logging details of accessing, changing, and editing the Source Codes as necessary for investigation purpose.

9. Use of Privileged Utility Programs

9.1 The Information Responsible Unit should limit users and user's rights to System Utility Programs on Server as necessary.

9.2 The Information Responsible Unit which responsible for users' computers shall limit users and user's rights to System Utility Programs on users' computers as necessary.

Topic 6

IT Operation Management

1. IT system work procedures shall be established.

2. Licensed software from sources which are free from malware intruding against software installation on networks shall be used. The installation shall be done by adhering to the determined procedure.

3. A loophole monitoring team and security patch management team shall be established. The scope of responsibility shall cover result follow-up, risk assessment, and system patch operation.

4. A security baseline shall be established as a standard for configuration hardening. During the installation or patch update, the configuration shall be set as determined.

5. During every system change, installation settings, system data, hardware, software, firmware, and files, such as network diagrams, shall be recorded in order to ensure that there is updated information that can be used for accurate and prompt management against incidents that affect the IT system.

Topic 7

Password Management

1. Control, management, and security of the passwords stored on the Company's IT system shall be done.

2. Users shall set passwords which are difficult to guess. The password shall consist of upper case, lower case, numerals, and symbols, and shall not be shorter than 8 letters. It shall be kept as personal confidential data and shall not be disclosed to others without appropriate reason.

3. In cases where it is required to give passwords to another person, the user shall immediately change their password after the occasion ends.

4. The password reset interval shall be set as at least 90 days or as appropriate. Also, a temporary password shall be generated for limited usage periods and shall be deactivated after the period is over.

5. IT system User's password accounts and IT system administrator's password accounts shall be appropriately managed. Guidelines and records shall be done in written form and frequently reviewed.

6. IT system administrator's password safety improvement shall be considered for better security and coverage of current operation conditions and important IT usage. This can be done, for example, by using 2-factor authentication, a dual control where 2 personnel each possess part of the password, or storing passwords in a safe.

Topic 8

Third Party Access Control

1. Control procedures or measures for approval requests, connection patterns, system entry and exit records, and other operations shall be established. Also, the access rights shall be reviewed and verified in order to keep them up-to-date.

2. There shall be a procedure which controls the access requests to be approved only as appropriate. Also, usage logs shall be done in order for future inspection.

3. Prior to the access approval, agreement, records, and contracts regarding information confidentiality and non-disclosure shall be mutually done between the Company and third parties or external personnel; also, the third party or external personnel shall agree to adhere to the Company's IT security policy.

4. Services or contracts agreed with third parties or external personnel who work for the Company shall be inspected and frequently reviewed as appropriate. Also, the third party's service condition shall be revised when there is an IT system update or development, technology change, etc.

Topic 9

Use of Computer of Enterprise

1. All types of computers provided by the Company, such as desktops, notebooks, smart phones and tablets, are provided to the user as an essential tool used only for the Company's tasks. The user shall be aware of the responsibility for computer usage. They shall also understand and strictly adhere to such responsibility in order to prevent damage which may occur to the Company's resources or vital information.

2. All the Company's computers shall be controlled by the GPSC Group Digital Platforms division in order to achieve systematic management, security, and control of usage or access. This aims to allow an effective solution or operation command during emergencies.

3. All the computers provided to the user by the Company are the Company's resources. The user shall use such computers only for the Company's tasks. Usage or storage which may cause resource damage or loss shall be avoided. Also, the resources shall be maintained in a ready-to-use condition.

4. Users are not allowed to copy, change, or modify programs installed on the computer. All cases of hardware modification are not allowed as well.

5. Program installation, repair, parameter adjustments, or configurations done with the computer or program are allowed to be done only by the GPSC Group Digital Platforms division personnel or authorized personnel of the Company.

6. All the Company's computer must be required to proof of identity (Authentication) with the appropriate method. To access, sign-in shall always be required.

7. Users shall avoid storing essential work information only on the computer. Such information backup shall also be frequently done with other devices, such as shared drives, cloud, and external hard disks.

8. All computers provided to the users by the Company shall be equipped with cyber threat prevention programs or systems which can automatically prevent threats on a real-time basis. General users shall not be able to deactivate or cancel this program on their own.

Topic 10

Use of Mobile Device

1. Users are allowed to use the Company's or their own mobile devices, such as smart phones and tablets, to access or store the Company's information. Each user shall not use more than 2 mobile devices in total. If a higher amount is required, the user shall be allowed this only after approval by the GPSC Group Digital Platforms division manager or authorized personnel.

2. Personal mobile devices which the user uses with the Company's IT system or network shall not be equipped with security threatening software, such as Jailbreaking or Rooting, or unlicensed software. Also, the user shall strictly adhere to the policy established by the GPSC Group Digital Platforms division.

3. The GPSC Group Digital Platforms division shall be authorized for control, verification, suspension, and revocation of access; and deletion of information deemed harmful on the mobile devices, whether owned by the Company or the user, if the usage is deemed to be a risk to the infrastructure or the information in the Company's IT system.

Topic 11

Use of the Internet and Social Media

1. The GPSC Group Digital Platforms division shall procure devices, tools, or technology related to the internal internet system in order to allow such system to be effective and appropriate for the current circumstance. The procurement shall be done in compliance with the Computer Crime Act and the relevant laws.

2. Usage of security support devices, tools, or technology, such as Firewalls and Web Filtering Gateways, shall be promoted. This shall improve the safety of internet and online media access done via the Company's network.

3. The GPSC Group Digital Platforms division shall be authorized for control, verification, suspension, revocation, and record of the access to the internet, online media, etc.; such operations shall be lawfully done as appropriate.

4. Users shall not use the Company's internet or online media for personal business and shall not access inappropriate or threatening websites, such as unethical websites, national authority threatening websites, or malicious websites which are harmful to society.

5. Users who are not responsible for public relations tasks shall not disclose important business information or other corporate information to third parties or the public via the internet or online media without approval.

6. Users shall not distribute or transfer any information which is false, offensive to national security, related to terrorism, or an abuse of privacy; pornography; portraits, which a person did not give consent for sharing; or pictures which are created, edited, or amended electronically or by any other means in a manner which is likely to cause such other person to be defamed, denounced, detested or humiliated via the internet or online media.

Topic 12

Use of Email

1. Email shall be one of the essential communication channels of the Company. The GPSC Group Digital Platforms division shall control and maintain the email system for effective and secure operation. The division shall be authorized for usage inspection, suspension, revocation, record, and tracing done as necessary and appropriate.

2. Users shall use corporate email only for the Company's tasks and shall not be allowed to use such email for personal business. Also, users shall not be allowed to register or sign up for social media, which is not related to their duties or the Company's operation, with their corporate email.

3. Users shall carefully use their email in order to prevent any damage to the Company, abuse of copyright, irritation, abuse of laws, or unethical actions. Also, users shall not seek business benefits or allow other persons to seek such benefits by utilizing their email via the Company's network.

4. Users shall be responsible for keeping updated on security announcements, understanding, and strictly adhering to instructions. Users shall also read emails or open attachments with care. Before downloading an attachment, users shall check the sender's name, their email address, and the email content. If there is any suspect detail or abnormality, users shall immediately report to the GPSC Group Digital Platforms division for inspection and shall not proceed with any action before receiving explanation or suggestion from GPSC Group Digital Platforms division personnel.

Topic 13

Cryptographic Control

1. Important information being sent and receipted via public networks shall be encrypted with a method which meets international standards, such as SSL (Secure Socket Layer) or VPN (Virtual Private Network).

2. There shall be a measure controlling the accuracy of information being stored, inputted, operated, and outputted. In the case that a distributed database is utilized or there is storage of various sets of information which partly or fully share the same content, the accuracy shall be controlled and ensured.

3. Information security measures shall be put in place for situations where computers are carried outside the Company for various purposes, such as getting repaired. For example, information stored in the drive may be deleted.

4. Efficient Cryptographic Key Management is significant part of security for encryption system. Cryptographic Key management process shall ensure that only authorized users are able to access the encrypted data and decrypt such data. Through the designed control and data retention requirements, Cryptographic Key Management shall conform to the following clauses.

4.1 There shall be the process for system control in order to access the Cryptographic Key only for authorized users as necessary. There shall also be the segregation of duties of authorized users who can access the Cryptographic Key among other users. This control shall be applied to any authorized users whose duties are relating Cryptographic Key or to any users who are authorized to the securities areas where key cryptography is processing, including Certificate Authority (CA), Registration Authority (RA), and other service providers.

4.2 There shall be the process for inspecting the data backup areas of Cryptographic Key data and file, and configuration data in order to prevent the loss of encrypted data.

4.3 To ensure of the segregation of duties, Control of Cryptographic Key shall be based on Two-person control method, which requires at least 2 persons designated from different functions.

4.4 There shall be NO single individual authorized to access and create new Key Pair of Certificate Authority.

4.5 Logging data of Cryptographic Key shall be verified on a regular basis, at least 4 times in a year.

4.6 Employee or officers who are authorized to manage Cryptographic Key shall undergo and pass the criminal record checking.

4.7 Employee or officers who are authorized to manage Cryptographic Key shall be trained on the necessary courses relating to Cryptographic Key Management on a regular basis, at least once a year.

4.8 There shall be the Job rotation approach applied on Cryptographic Key on a regular basis, at least twice a year.

4.9 For Fully Automated Cryptographic Key Management, Employee authorized to manage the Cryptographic Key shall neither have any chance to get the direct access to the Cryptographic Key nor have any chance to create the new Key without authorization.

4.10 The Cryptographic Key shall be always encrypted both during stored in data storage devices and during data transmission.

4.11 Private Key used for accessing to Cryptographic Key shall be always stored with confidentiality and security.

4.12 Cryptographic Key shall be created through random method generating from the key space possibility by means of the key creating hardware.

4.13 The Key-encrypting key shall be different from the Data-encrypting key.

4.14 Using the Key with its key life longer than 2 years remaining shall be only in necessary cases with the approval of Digital Platform Division Manager (SGM) or any persons assigned from Digital Platform Division Manager (SGM).

4.15 The delivery of the Cryptographic Key to receiver shall be made only via the designed secure channel.

4.16 The device used for creating the Cryptographic Key shall be securely protected in both physical and digital way.

4.17 The Cryptographic Key shall be revoked immediately after founding that the Key is prone to risk, leading to security violation such as the private key was leaked out to other undefined persons.

4.18 The revocation of the Cryptographic Key shall be informed to all responsible persons and Key users of Key details, reasons for revocation, and the date and time of revocation. The revocation of the Cryptographic Key shall be acceptably made via Online Certificate Revocation List (CRL).

4.19 Any actions relating to the Cryptographic Key shall be securely recorded as Log data in order to serve traceability purpose.

4.20 For the Cryptographic Keys which have not been in used for too long, archiving such Keys shall also be made through encryption in a secure way.

4.21 Archiving the Cryptographic Keys, or Key recovery, shall be made as a plan for inspection which is contained in business continuity plan.

4.22 Disposing Cryptographic Key shall be meticulously performed in a secure way. There shall also be ensured that no need for using the disposed Key to use in the future anymore.

Topic 14

Physical and Environmental Security

1. The area where security is required shall be determined. Appropriate separation and determination of IT system operation areas will facilitate monitoring, control, and security against unauthorized persons. In order to reduce risks and prevent damage caused by any disaster, such as a fire, flood, earthquake, terrorist attack, etc., additional procedures shall be put in place.

2. IT system operation areas shall be clearly determined and identified. The layout of such area shall be established and widely announced. The area may be determined as: general operation area, administrator area, device distribution area, etc.

3. Computer centers shall be separated from the general operation area as a separate room. Entry and exit of the security area shall be restricted only to the responsible or authorized personnel.

4. Computers, networks, servers, intrusion prevention systems, and other security systems shall be maintained frequently or according to the interval suggested by the producer.

5. Procedures on operation, storage, destruction, and access control of information, information storage devices, and IT resources shall be appropriately established.

6. The personnel responsible for physical and environmental security activities shall be assigned with clearly determined duties and responsibilities.

Topic 15

Malicious Software Protection

1. The Company and its Information Responsible Unit division shall use software equipped with malicious software detection and protection. All employees shall adhere to this policy and shall not install software on their own without approval of the administrator or authorized personnel.

2. Portable storage devices, such as USB, CD, and DVD, are not allowed to be used with the ICS. If there is any necessity to do so, approval shall be obtained, and a cybersecurity risk assessment shall be done.

3. There shall be measures preventing malicious software from portable storage devices, such as USB, CD, and DVD, from disseminating into the computers used for business operation. Usage of portable storage devices shall also be monitored.

Topic 16

Change Management

1. IT system security and operation change control procedures or measures shall be established. This is to ensure the accuracy of all change processes and compliance with users' needs; and to ensure that the important information is changed in an orderly and appropriate manner. The procedures and measures shall cover all the change processes, from change requests until the utilization of the changed IT system.

2. All improvement or change processes shall be considered in compliance with cybersecurity, data privacy and authorization, and availability.

3. Control procedures or measures on all IT system change details, such as configuration and source code, shall be put in place in order to provide an operation standard and allow appropriate tracing done according to document or information versions.

4. Developing environment and testing environment systems shall be separated from the actual system in order to prevent information access or actual system changes done by unauthorized personnel. Also, IT resource operation condition tracing and capability analysis shall be frequently done.

5. Change acceptance criteria shall be established and the newly changed system shall be inspected before being accepted in written form.

6. Before execution (Go-Live), any change being done to the actual system or affecting the users' operations shall be announced to all the relevant users.

Topic 17

Network Access Control

1. There shall be network access control measures, for both wired and wireless networks. Physical sorting and user authorization shall be done in order to ensure the compliance of access rights with users' responsibilities. There shall be authentication done before connecting to the wireless network of which access is only allowed for authorized personnel.

2. The GPSC Group Digital Platform division shall procure devices, tools, or technology for facilitating or controlling network access to be effective and appropriate for the current circumstance. Also, the GPSC Group Digital Platform division shall provide security devices, tools, or technology in order to enhance safety in network usage and access.

3. Control procedures or measures shall be put in place in order to prevent network access from outside of the organization; for example, remote access done via the internet.

4. The GPSC Group Digital Platform division shall be authorized for control, inspection, suspension, revocation, and record of the Company's network usage and access done as necessary and appropriate.

5. Installation, modification, and change of any device, connector, or software used with the Company's network shall be done only under the authority of the GPSC Group Digital Platform division.

6. Company's network device registration shall be done. Measures on access control, parameter determination, and maintenance of devices or systems used with the Company's network shall be established. Also, such registration and measures shall be frequently updated as appropriate.

7. There shall be a measure controlling the usage of LAN ports to be allowed at necessary areas. Wireless access points shall be placed at areas suitable for a working space. The signal shall be prevented from being distributed to outside the determined area, or an area where outsiders can hack the signal and damage the network.

8. Wireless network security standards, including device authentication, signal encryption, safe access controls, and device connection records, shall be put in place.

9. There shall be appropriate intrusion detection and prevention device and process. Unauthorized network access records shall be done in order to be analyzed for prevention development.

Topic 18

Information Exchange Management

1. The information exchange channels used in the Company' information system are as follows:

1.1 Email: to contact the Company's business email address, under domain names that consist of the names of GPSC or its affiliates' abbreviation, including @gpscgroup.com, @chpp.co.th, and ; or email addresses under the domain of the outsourcing company assigned by the Company shall be used.

1.2 Online storage, which requires the user to sign-in with the same account or user id used with the Company's information system for authentication, such as File Sharing, One Drive, SharePoint, etc.

1.3 Created, procured, or rental business applications, of which usage is officially announced, under the responsibility of the Information Responsible Unit.

1.4 Websites under domain names that consists of the Company's name or abbreviation, such as gpscgroup.com, chpp.co.th, etc. Such websites might be created, procured, or rented; and shall be under the responsibility of the Information Responsible Unit. Also, their usage shall be officially announced.

2. Employees and personnel of all levels who use the Company's information system shall exchange information only via the channels stated in 1.

3. Information exchange done via other channels in the system which are not stated in this policy shall be approved by the GPSC Group Digital Platform division manager in written form.

4. Management processes, work procedures, and control measures shall be put in place in order to ensure appropriate and effective information exchange and policies on distribution of the Company's information.

Topic 19

Cloud Security Management

1. Cloud Security Management on Cloud Service Provider:

1.1 There shall be inquiry about service details from Cloud Service Provider to use for selecting and evaluating its service, which shall be at least as follows:

1.1.1 Electronic commerce: Information System Owner shall develop Information System which provide Electronic commerce service via secure public networks, which meet the relevant laws and procedures in order to prevent from frauds and unauthorized access to and edition on the data.

1.1.2 Cloud Security measures applied on Cloud Service Providers, including SaaS Service shall also take into consideration the security measures on system development process performed by Cloud Service Provider.

1.1.3 Cloud Security measures shall cover the Cloud Service Provider applied on the sharing Company's information assets or sharing internal management process with other clients than Company.

1.1.4 There shall be certificate of Cloud Security Management which met international standard for Cloud Service Provider such as ISO/IEC 27017 and Cloud Security Alliance (CSA STAR), including the inspection evidence documents on Cloud Security such as inspection report, Cybersecurity control measures report, Information Security control measures report which are used for certification assessment, etc.

1.1.5 All compliance with relevant laws and regulations for Cloud Security performed by Cloud Service Provider which affects Cloud Service provided to Company shall be taken into consideration the Cloud Service Provider location which store, transmit, and process Company's data.

1.2 There shall be defined duties for Cloud Security Management performed by Cloud Service Provider. The segregation of duties on Cloud Service Provider and Company shall be apparently specified in the contract. At least, there shall be the access control for data access, information asset management, and information asset maintenance.

1.3 The Company's information asset list relating to Cloud Service shall be made with the following details:

1.3.1 Define Data Owner of data stored on Cloud, including system logging.

1.3.2 Define responsible persons managing information assets (Company or Cloud Service Provider).

1.3.3 Locate the country which the Cloud Service Provider's computer center used for storing, transmitting, and processing the Company's Information Asset of Cloud Service Provider locates.

1.3.4 List of Information asset and information which the Company grant the access right to Cloud Service Provider.

1.3.5 Labeling the Company's information asset and information as identify on the asset list.

1.4 Training courses on Information Security Awareness shall be conducted for Management, System Users, System Administrators, and relevant persons. The trainings shall cover process for Cloud Service operation, risks and risk control measures on Cloud Security, and laws and regulations on Cloud adopted from external regulators.

1.5 There shall be the analysis of data quantity usage on Cloud, trend in the Cloud usage, planning for resources relating to Cloud, and duration of Cloud Service usage in GPSC.

1.6 There shall be the consideration of data backup and retrieval methods in case there is any change or termination of Cloud Service contract.

1.7 Customer data and data classified as and more "Confidential" level stored in Cloud by Cloud Service Provider shall be manage through Masking, Render, Token or Fragmentation in order to reduce the data confidentiality level and to reduce risks of data disclosure. Thus, for data classified as and more "Confidential" level, there shall be Data Encryption during both data storage and data transmission in accordance with the Company relevant standard.

1.8 There shall be business continuity plan for emergency or disaster in case that Cloud Service Provider cannot provide service to the Company. The business continuity plan shall be tested by both Cloud Service Provider and the Company in order to ensure RTO (Recovery Time Objective), RPO (Recovery Point Objective), and MTPD (Maximum Tolerable Period of Disruption) are met as defined by the Company. The business continuity plan shall take into consideration the location of computer center which store, transmit, and process the Company's information asset.

1.9 There shall be the risk assessment on Cloud Service, including Cloud Computing performed by Cloud Service Provider. The risk assessment should cover the risks relating to Confidentiality, Data Privacy Protection, Dependency on Cloud Service Provider, which lead to the difficulty in changes or termination of service contract (Vendor Lock-in) and the impact on the Company's work system. In addition, in case that the Company's uses Cloud Service, especially data storage, computing, or any service related to the Company's data, from Cloud Service Provider from overseas country, there shall be the assessment of the risks on the country which the Cloud Service Provider locates such as the Service Interruption, Communication Network Blocking, Information Access Risk, and Cross-border Compliance.

2. Cloud Service Provider shall provide Cloud Security Management to comply with both the Company relevant policies and standards, and relevant laws and regulations, which shall be at least as follows:

2.1 In case that the Company's uses Virtual Private Cloud provided by Cloud Service Provider, there shall be the Network Isolation for the Company out of the network system provided for other Cloud Service clients.

2.2 There shall be the Access Control System on Network System for Cloud Service provided for the Company by limiting the access rights as necessary, in accordance with the defined duties.

2.3 There shall be the system for managing user accounts provided for Cloud Service Provider to manage access rights for all users as necessary, in accordance with the defined duties and usage reasons.

2.4 There shall be the authentication system with security provided for the Company to be able to select the appropriate method among various methods responding to the important level of the Company's data such as Multi Factor Authentication, and compatible with other systems used in the Company.

2.5 There shall be the encryption system for data classified as and more "Confidentiality" level which are stored, and transmitted in Cloud. There shall also be the testing on encryption provided by Cloud Service Provider to ensure the compatibility with other systems used in the Company.

2.6 The Key Management Service System shall be established, available, and managed by either the Company or Cloud Service Provider. The key shall be kept only by the Company.

2.7 There shall be the Data Disposal process and the Device Reuse process defined by Cloud Service Provider with security. When the termination or the cancellation of Cloud Service are effective, Cloud

Service Provider shall be required to store relevant data for the Company for at least 30 calendar days, based on the data quantity stored in the Cloud, in order for the Company to complete data migration.

2.8 If Cloud Service Provider requests for cancel partial or entire the Cloud Service, Cloud Service Provider shall inform the Company of such request at least 1 year in advance.

2.9 There shall be the change management process relating to the Company's Change Management Process for Information. In case Cloud Service Provider makes any changes affecting Cloud System provided for the Company, Cloud Service Provider shall inform GPSC before making such changes in order for the Company to conduct the Company's Change Management Process for Information on such change, including assess the business impact.

2.10 There shall be the resource monitoring on Cloud Services performed by Cloud Service Provider. Cloud Service Provider shall take responsibility for resource management, and immediately inform the Company of resource when resource scarcity is found or the resource quantity reaches the threshold as defined by the Company. Cloud Service Provider shall also submit the resource usage report to the Company on a regular basis.

2.11 There shall be Logging records and Clock Synchronization on Cloud system with enough space for storing Logging records as defined by the Company.

2.12 Cloud Service Provider shall be the inspect Cloud Security on a regular basis, and submit the inspection summary report to the Company at least once a year.

2.13 The Company shall be authorized to access, inspect, and retrieve the data from Cloud Service Provider, including data relating to its Sub-contract. In case Cloud Service Provider cannot allow the Company to access and inspect the Cloud system, Cloud Service Provider shall submit data evidence to the Company enough for performing inspection or submit the inspection result performed by the external independent party as required by relevant international standards.

2.14 There shall be the Security Incident Management. Cloud Service Provider shall report security incident to the Company immediately, and also submit Security Incident Summary Report to the Company at least once a month.

2.15 There shall be Forensic Process, in case of Cloud Security violation. There shall also be the data collection process for gathering important evidences necessary for legal proceeding.

2.16 There shall be business continuity plan, in case of emergency or disaster to serve the case that Cloud Service Provider cannot provide service to the Company such as Communication Network Blocking. There shall also be the testing of business continuity plan and submit the testing report to the Company at least once a year.

3. Cloud System Administration or System Developer shall execute Cloud Security Management, at least they shall:

3.1 perform the technical Cloud Security Management affecting the Company's service system such as Security Baseline, VA, Penetration Testing, Patch.

3.2 monitor main resource usage, and inform Management of resource scarcity is found or reach the threshold as defined by the Company.

3.3 control the use of copyright software in Cloud system by inspecting before usage, and also considering the capability of using expansion in the system and processing units, including the numbers of processing units which might be greater than the numbers of copyrights earlier prepared.

3.4 in case using Container, prepare and improve Container Image used in Cloud every time of changes.

3.5 obtain business continuity plan. In case of emergency or disaster and case of disability to provide service to the Company, there shall be the co-testing on the plan with Cloud Service Provider in accordance with the defined RTO (Recovery Time Objective), RPO (Recovery Point Objective), MTPD (Maximum Tolerable Period of Disruption) by considering the Computer Center used for storing, transmitting, and processing the Company's Information Asset.

Topic 20

Systems acquisition, development and maintenance

1. Requirements for Information System Security

To ensure that requirements for Information System Security defined appropriate ranging from system procurement to system development, the requirements are stated as follows:

1.1 There shall be the identification and analysis of requirements for Security. Information System Administrator shall define the requirements for Information System Security when there is a new procurement for Information Security or when developing the existing Information System.

1.2 Security for programs available on public network, and Protection of Right and Intellectual Property

1.2.1 Electronic commerce: Information System Administration shall develop Information System provided for Electronic Commerce via public network in accordance with the defined standards and compliance with the relevant laws and regulations in order to prevent frauds, including to protect the Company against unauthorized access and edition on important information.

1.2.2 Publicly available information: Information Owner shall control the publicly available information based on accuracy, integrity, and compliance with the relevant laws and regulation.

1.3 Protection of Information Transactions: Information System Administration shall develop the information system provided for online transactions with the security measures meeting the defined standards and compliance with the relevant laws and regulations in order to meet information completeness and to prevent spoofing.

2. Security for Development Process and Support Process

2.1 System Development with Security

2.1.1 There shall be the security embedded into SLDC by defining analysis, planning, or creating security measures in each phase of SLDC and also conform to the Company's SLDC.

2.1.2 Requirements for Information System Security shall be defined.

2.1.3 Information System provided service via pubic network (e.g., Internet) should be taken the Risk Assessment with Risk Mitigation Plan.

2.1.4 Information System should be designed based on Secure Software Development Principles.

2.1.5 Software Development shall be performed through secure methods.

2.1.6 During the development of System, there shall be the identification of Security Checkpoint in order to ensure the Controls for Security are developed to respond to the defined requirements for security. For example, reviewing Source Codes (Security Code Review) is conducted before entering Software Testing.

2.1.7 Any problems found during the development phase shall be informed to Project Manager or Supervisor. As a result, the problem shall be solved and recorded.

System Developer shall be trained on Security for Development and/or knowledge relating to Information Security threats on a yearly basis.

2.2 There shall be the procedure for control of changes or editing the System. The control shall ensure that any changes affecting the System are required approval and supervision from the authorized persons as defined in relevant standards before making any changes.

2.3 The testing on the System functioning shall be conducted when Operating System is changed. System Administration and the testing working party shall together review and test the System functioning whenever the changes in Operating System is made in order to ensure there is no effect on the System Security.

2.4 Any changes in package software shall be approved and controlled in accordance with the defined standards before making changes.

2.5 Secure System Engineering Principles shall be defined in order to make reliability, meet the appropriate security levels, and meet the Company's business requirements.

2.6 There shall be the secure Development Environment. There shall also be the preparation and protection for the Development Environment covering all SLDC with security measures as follows:

2.6.1 The segregation of duties among Development Environment, Testing Environment, and Production Environment.

2.6.2 The control measures which allow only authorized persons to access the Development Environment.

2.6.3 Protection of the data stored and processed in the Development Environment, and data transmitted between Development Environment and Production Environment.

2.6.4 The strict inspection and control of data transmission in and out the Development Environment.

2.6.5 Data Backup for all important data, such as Configuration data, Source Codes, Development documents, User Manuals, in the secure specific area out of Development Environment.

2.7 Outsourced Development: Organization units making the outsourcing shall define the requirements for Software Security and control the Contractor to follow the defined standards.

2.8 System Security Testing

2.8.1 There shall be the testing on the developed System or the changed System before acceptance and use.

2.8.2 The testing shall be performed by the working party consisting of representatives from relevant Departments.

2.8.3 The testing shall be conducted in the nearest or virtual Production Environment. The testing shall follow the same security measures as defined in the Development Environment.

2.8.4 The testing shall be completely separated from the Production Environment in order to prevent any impacts might happen during the testing.

2.8.5 The testing shall include all testing topics to ensure that the developed or improved System meets the requirements for Function, Capacity, and Security aspects.

2.8.6 The inspection on the main System (e.g., System functioning via public network) shall be conducted through Vulnerability Scanning and/or Penetration Test in order to discover the system flaws which, subsequently, shall be solved appropriately.

2.9 System Acceptance Testing

2.9.1 Organization units making the outsourcing shall define requirements for Information System Security and requirements for business continuity in accordance with the relevant standards.

2.9.2 Persons who perform System Acceptance Testing shall perform the tasks in accordance with the requirements for Information System Security and requirements for business continuity.

3. Test data

In order to ensure that the Test data is appropriately utilized for the testing with protection for security, persons performing the testing and System Administrator shall perform as follows:

3.1 The Test data shall be approved by Data Owner before performing the testing.

3.2 The Test data shall be converted to confidential data in the Developed System before conducting the test and shall be destroyed after completing the test in order to prevent the data from leakage during the test.

3.3 There shall be the control of accessibility to the Test devices with security measures equivalent to the System in Production Environment.

Topic 21

IT Outsourcing Management

1. IT outsourcing management procedures or measures shall be put in place. The contents shall cover service provider selection, engagement, quality control, access rights, verification, service acceptance inspection, and performance evaluation in order to ensure that these operations are proceeded appropriately, all terms and conditions are performed, and no damage will occur against the Company's information and information system.

2. Allowance of other service providers to access the Company's information and system shall be done in accordance with security policies and relevant information protection policies. The Information Responsible Unit division manager shall hold the authority to approve the access or authorize responsible personnel to perform the approval as appropriate. The approval shall be done in written form or recorded for traceability.

Topic 22

Information Security Incident Management

1. Information security incident communication channels shall be clearly identified.

2. If users notice any information security incident, they shall immediately report to the GPSC Group Digital Platforms division.

3. Information security incident reports shall be done according to the severity level of the incident. If the incident is severe and may affect many users, it shall be promptly reported.

4. Security incidents shall be recorded. As minimum information, the type of incident, number of occurrences, and damage cost shall be recorded and learned in order to develop preventive action.

5. Evidence shall be gathered and stored in accordance with rules or regulations as a reference used in legal process.

6. Information security incident management plans and recovery plans shall be put in place in order to reduce the impact and recover business and manufacturing operations.

7. Information security incident management plans and recovery plans shall periodically be tested in order to check their efficiency and effectiveness. If any point requires improvement, such improvement shall be finished within 1 month after the test.

Topic 23

Backup and IT Continuity Plan

1. The Information system shall be divided into groups for prioritization. Procedures or measures on information system management, backup, recovery, storage, and preparation for emergencies shall be established in accordance with importance level in order to ensure that the most important information and information system of the Company will always be available and can be effectively used when they are needed.

2. There shall be a procedure and measure put in place for backup result inspection, general and emergency information recovery tests, and tests on the most important information system in order to appropriately prepare for emergency situations.

3. Processes of backup, recovery, storage, and preparation for emergency in every importance level shall be reviewed and improved in order to ensure their efficiency.

4. Information backup device storage sites shall not be the same as the site where the system is located. Entry and exit of such sites shall be restricted and physical security systems shall be equipped. Control and verification measures for the discontinuation or destruction of backup devices shall also be established.

5. In the case that the GPSC Group Digital Platforms division is not responsible for some or all of the processes, outsourcing management measures shall be established and applied to the service provider. The measures shall cover engagement, quality control, verification, and performance evaluation.

6. Business continuity management related information system operation processes and procedures shall be established in accordance with business continuity management in order to effectively manage incidents.

Topic 24

IT Audit Logging

1. Information system usage and users' activities shall always and appropriately be recorded as required by the law or the Company's security policy. However, the operation shall not be contradictory with personal data protection policy.

2. Information system usage record protection measures shall be put in place in order to prevent unauthorized access. Operations of the personnel related to such system shall also be recorded.

3. The relevant errors shall be recorded, analyzed and solved as appropriate.

4. Information system usage and users' activities record shall be stored for an appropriate period of time in order to facilitate the inspection done by the GPSC Group Digital Platforms division or the Digitalization Strategy or other division authorized by the Chief Executive Officer when there is any system security incident or abuse of law or the Company's policy noticed or suspected.

Section 25

Compliance

1. Compliance with laws and contracts

In order to reduce risks of violation of laws and procedures relating to the Company's business, to meet the compliance, and to prevent from violation loss, there shall be requirements as follows:

1.1 Identification of legal-binding requirements

1.1.1 Organization unit responsible for Risk Management shall collect and update legal-binding requirements, including relevant procedures. The awareness of risks and relating legal-binding requirements shall be built in all organization units

1.1.2 All organization units shall follow legal-binding requirements and relevant procedures relating to their own duties.

1.2 Right and Intellectual Property Protection

1.2.1 Organization units responsible for Information Technology assets shall keep the evidences of copyright software and shall make the list in order to control the numbers of users not to exceed the right.

1.2.2 Users shall use only the copyright software for performing their tasks.

1.3 Logging record Protection

1.3.1 Persons who possess the Company's Logging records relating to legal-binding and business requirements shall appropriately manage, store, and destroy Logging records. There shall also be the prevention of Logging records from loss, destruction, deception, and misuse.

1.4 Personal Data Protection

1.4.1 Personal data of customers and employees in both document and electronics data shall be treated as confidential. Disclosure of any personal data shall be required approval only from personal data owner.

1.5 Rules for data encryption

1.5.1 System Administrator shall define the encryption for important data which considered as confidential data for the Company, and comply with legal requirements and relevant the Company's procedures relating to doing business.

1.5.2 System Administrator shall develop the encryption for important information which treated as confidential both during the data transmission and data storage to comply with legal requirements and relevant the Company's procedures relating to doing business.

2. Review of Information Security

In order to ensure that the information security is implemented accurately, completely, appropriately and conforming to relevant policies and procedures, there shall be requirements as follows:

2.1 Verification of Information Security by external independent party.

2.1.1 Organization unit responsible for regulating Information Security shall verify the compliance with relevant policies in order to support making the development of Information Security in the Company, including report the verification to Risk Management Committee.

2.2 Compliance with relevant policies and standards

2.2.1 All relevant employees shall perform duties complying with relevant policies and standards.

2.2.2 The Company's Executives shall govern employees in their reporting line to follow relevant policies and standards

2.3 Compliance check on technical requirements

2.3.1 Personal data of customers and employees in both document and electronics data shall be treated as confidential. Disclosure of any personal data shall be required approval only from personal data owner.

2.3.2 Organization units responsible for governing Information Security shall randomly conduct compliance checks on the technical requirements and system vulnerability in order to ensure compliance with relevant policies and standards.

2.3.3 Software Tools used in inspection or testing the compliance with technical requirements and system vulnerability shall limit the access rights granted only to authorized persons who perform such tasks.

Section 3

Information System's Environmental Friendliness Policy

GPSC and its affiliates determine the ICT system to be a vital element for business support and performance improvement. Importance and attention are placed on the protection of employees, properties, business information, and positive reputation of GPSC. However, the ICT devices currently used may cause negative effects to the environment. Thereby, GPSC has determined the information system's environmental friendliness policy which is as mentioned below.

1. Efficient Energy Use

Use ICT devices and other relevant devices of which eco-friendliness is certified by international accredited organizations, such as Energy Star or EPEAT.

2. Device Selection and Management

Select ICT devices made from material which is not harmful to human and environment. When they are no longer used, the devices shall be correctly discarded or destroyed without environmental impact in accordance with widely accepted standards.

Use environmental friendly ICT equipment that has been audited to assess the impact of the production process throughout the product lifecycle from an environmental specialist according to the criteria or requirements of each product type as a "label" or "marked" issued by the agency of certificate in Thailand or abroad or certified according to ISO 14020 (Environmental Labels) such as "Green Label", "EU Eco-Label", "Green Seal".

3. ICT Waste Management

Usage of consumables shall be reduced. The consumables may be reused as appropriate. If reuse cannot be done, they shall be correctly discarded or destroyed without environmental impact.

Section 4

Good Information and Communication Technology Governance Policy

In order to make the ICT operations of GPSC and its affiliates compliant with laws, regulations, and international standards; and allow continued development done in accordance with GPSC's risk management and PTT's policy, a good Information and Communication Technology governance policy is established as mentioned below

1. ICT cooperation shall be encouraged among the PTT Group, focusing on usage of the mutual services, in order to share resources and knowledge, enhance ICT system security, and facilitate performance improvement.

2. The operation shall be done in accordance with privacy policies, concrete information security management, and the relevant information technology laws in order to comply with laws, regulations of the government sectors, or the Company's policies.

3. Consideration to bring the ICT to support internal and external operations for consistency and continuity of operations in all important systems. To facilitate business sustainability, ICT sustainability shall be achieved. Also, the prevention of impact and loss against stakeholders, properties, and information of the Company shall be done by determining process control points and verifying and monitoring important operations in all processes frequently and appropriately.

4. Information technology risk management will be appropriately done in accordance with the Company's business operations and frequently reviewed.

Regulations shall be applied with and understood by all departments, management, employees, and personnel of GPSC. The management at all levels shall act as role model and encourage strict implementation. Also, implementation evaluation shall be done by an independent division in order to ensure that all the relevant employees and third parties comply with this regulation.

This regulation shall come into force on September 1st , 2021.

Announced on 25 August 2021

(Mr. Worawat Pitayasiri)

President and Chief Executive Officer