Global Power Synergy Public Company Limited's

Regulations on Information and Communication Technology Policy Standard Practice

2020

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

Section 2 Information Security Policy

Section 3 Information System's Environmental Friendliness Policy

Section 4 Good Information and Communication Technology Governance Policy

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

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. Security Principles

These security principles aim to achieve the following purposes:

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

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

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

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

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

3.6 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

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

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

- All employees and relevant external personnel shall be responsible for security.
- Security management and operations shall be continuously done.
- 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.

4. 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.

5. 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.

6. Terms and Definitions

"GPSC" or "Company" means Global Power Synergy Public Company Limited.

"Chief Executive Officer" means the chief executive officer of Global Power Synergy Public Company Limited.

"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.

"Commander" means an authorized person according to the organizational structure.

"System Administrator" means a person who is assigned by the commander to maintain the computer system and network. The system administrator can access the computer system program in order to manage the network database.

"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 tool" means a tool or a set of tools 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.

" Information" means the data, news, records, history and text in a document, computer program, computer data, picture, audio, sign, or symbol stored in a form which can be directly understood by a person or displayed via device or tool.

"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 and Intranet" 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 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.

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 The Information and Communication Technology security management policy and other relevant policies shall be established in order to achieve trust and security in Information and Communication Technology system usage as well as to allow 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.

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

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 President

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 Chief Information Officer Who Also Holds the Position of Chief Information Security Officer

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 Information or Information System Owners

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 Personnel of Information Technology Division

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. 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 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 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 immediately 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 IT division. Also, the labels attached on documents and IT resources for clear identification shall be appropriately defined.

2. 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 IT division 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. Appropriate procedures or guidelines on resource usage shall be established 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 IT division manager or the employee assigned by such manager 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 annually.

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 IT division 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 annually.

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 PI networks 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 IT 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 annually.

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. Services, such as telnet

FTP or ping, 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 IT 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 IT 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 IT division manager or authorized personnel.

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. Operator accounts and IT system administrators account shall be appropriately managed. Guidelines and records shall be done in written form and frequently reviewed.

6. 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, and surfaces, 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 IT 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 IT division personnel or authorized personnel of the Company.

6. To access the Company's computer, 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 smartphones, tablets, and iPads, 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 IT 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 IT division.

3. The IT 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 IT 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 IT 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 IT 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 IT division for inspection and shall not proceed with any action before receiving explanation or suggestion from IT 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.

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 IT 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 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 and testing 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, 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 Company's IT division shall procure devices, tools, or technology for facilitating or controlling network access to be effective and appropriate for the current circumstance. Also, the IT 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 IT 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 IT 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 8

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 @glow.co.th; 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 IT division

   1.4 Websites under domain names that consists of the Company's name or abbreviation, such as gpscgroup.com, chpp.co.th, glow.co.th, etc. Such websites might be created, procured, or rented; and shall be under the responsibility of the IT division. 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 IT 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

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 promised service 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 IT 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 20

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 IT 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 21

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 IT 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 22

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 IT division or other division authorized by the President when there is any system security incident or abuse of law or the Company's policy noticed or suspected.

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.

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 PPT's policy, a good Information and Communication Technology governance policy is established as mentioned below

1. ICT cooperation would be encouraged among the PPT 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 would 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. ICT may be used 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 December 14th, 2020.

Announced on December 2020

(Mr. Worawat Pitayasiri)

President and Chief Executive Officer