**Company Regulation: Global Green Chemicals Public Company Limited**

**Information Technology Security Policy, B.E. 2565 (2022)**

---

**Purpose**

To ensure the information systems of Global Green Chemicals Public Company Limited and its affiliates are secure, operate continuously and efficiently, and comply with ISO/IEC 27001 or other international standards. The policy also aims to raise awareness and establish preventive measures against threats from improper use of information systems, and to ensure compliance with relevant laws such as the Computer Crime Act B.E. 2550 (2007), Cybersecurity Act B.E. 2562 (2019), Personal Data Protection Act B.E. 2562 (2019), and other applicable laws.

**Article 1**

This regulation is called the "Information Technology Security Policy, B.E. 2565 (2022)" of Global Green Chemicals Public Company Limited.

**Article 2**

This regulation is effective from October 1, 2022, onwards.

**Article 3**

This regulation repeals the previous Information Technology Security Policy, B.E. 2563 (2020).

---

**Chapter 1: General Provisions**

**Article 4: Definitions**

**4.1** **Company**: Global Green Chemicals Public Company Limited.
**4.2** **Affiliates**: Companies or legal entities in which the company holds shares directly or indirectly.
**4.3** **User**: Authorized users of the company's information systems and networks.
**4.4** **Executives**: Executives from department manager level and above.
**4.5** **Employees**: Employees of the company and its affiliates assigned to perform duties.
**4.6** **Contract Workers**: Legal entities or representatives contracted to work for the company.
**4.7** **Interns**: Students authorized to intern with the company or its affiliates.
**4.8** **System Administrators**: Individuals assigned to manage and control the company's information systems or networks.
**4.9** **ServiceDesk Staff**: Personnel responsible for advising or resolving user issues with information systems.
**4.10** **IT Department**: The department responsible for managing the company's information systems.
**4.11** **Responsible Department**: Departments assigned by executives to perform specific tasks.

**4.12** **Data/System Owners**: The party authorized by a supervisor to be responsible for operational data, where the data owner is responsible for such data or is directly affected should such data be lost.

**4.13** **External Parties**: External entity that is authorized by the Company to access and use the Company's information or assets. Such parties shall be granted access rights in accordance with their authorized roles and responsibilities and shall be responsible for maintaining the confidentiality of the Company's information in accordance with a confidentiality agreement.

**4.14** **External Cloud Providers**: An external unit that provides services in the form of a cloud system.

**4.15** **Computer**: Data processing devices operating through an OS, including CPU, monitor, and keyboard.

**4.16** **Mobile Device**: Easily portable devices with an OS, capable of input, display, and network access (e.g., smartphones, tablets, notebooks).

**4.17** **Personal Mobile Device**: User-owned portable devices connected to the company's systems.

**4.18** **Network Device**: Devices used to connect computers or networks for data exchange.

**4.19** **Computer Data**: Data, text, commands, or other items in a computer system, including electronic data as per e-transaction laws.

**4.20** **Information System**: Systems, computers, networks, and devices providing company information services.

**4.21** **Information**: Facts processed and organized for easy understanding and use in management, planning, decision-making, etc.

**4.22** **Information Data**: Data, text, images, or other items related to company business, in electronic or print form.

**4.23** **Personal Data**: Information that can identify a person, directly or indirectly, excluding deceased persons.

**4.24** **Data at Rest**: Data stored on company media such as share drives, file servers, databases, or user computers.

**4.25** **Computer Network**: Connections between computers and network devices for shared information exchange.

**4.26** **Social Network**: Systems enabling communication and information sharing via the internet using social media technology.

**4.27** **Assets**: Computer data, information systems, and IT assets such as computers, company mobile devices, network devices, and licensed software.

**4.28** **Security Incident**: Events potentially causing damage or loss to the company, its personnel, or assets, including information leaks.

**4.29** **Standard**: Benchmarks enforced in actual operations to achieve objectives.

**4.30** **Procedure**: Detailed steps to achieve the set standards.

**4.31** **IT Security Management System**: The administration and management of information systems in order to create security, considered based on risks relating to the Company's information assets, by determining measures and implementing a risk-reduction plan, including regularly reviewing and improving such risks and processes.

**4.32** **Computer System**: A device or set of devices of a computer that are linked to operate together, in respect of which commands, sets of commands, or other matters and operating guidelines have been established so that the device or set of devices automatically performs data processing.

**4.33** **Network System**: Systems for communication or data transfer between company information systems (e.g., LAN, Intranet, Internet).

**4.34** **LAN/Internet**: Electronic networks connecting computers within a department for communication and information exchange.

**4.35** **Internet**: Electronic network connecting company networks to the global internet.

**4.36** **Cloud System**: Information systems providing shared services over computer networks.

**4.37** **IT System Workspace**: Areas authorized for information system use.

**4.38** **E-mail**: A system that people use to send and receive messages to one another via computers and interconnected networks. Data sent may be in the form of text, photographs, graphics, animation, and sound. The sender may send messages to a single recipient or to multiple recipients. Standards used for transmitting this type of data include SMTP, POP3, and IMAP.

**4.39** **Password**: Characters or numbers used for identity verification and access control.

**4.40** **Malicious Code**: Code causing damage, destruction, alteration, malfunction, or deviation from intended operation.

**4.41** **Server**: Main computer in a network controlling other computers and storing programs/data.

**4.42** **Removable Media**: Storage devices that can be detached from computers while operating (e.g., hard drives, USB drives).

**4.43** **Phishing**: A form of cyber threat, typically taking the form of a forged e-mail or a website created to deceive a victim into disclosing financial information or other personal information, such as a credit card number, username, password, or national identification number..

**4.44** **Cyber Threat**: Any unlawful act or operation using a computer, computer system, or malicious program, intended to cause harm to a computer system, computer data, or other related data, and constituting an imminent danger likely to cause damage to, or affect the operation of, a computer, computer system, or other related data.

**4.45** **Jailbreak/Root**: Modifying the operating system of a personal mobile device so as to enable the installation of software that has not been verified by the owner of the operating system.

**4.46** **Application**: A set of commands written to cause a computer to operate for a specific purpose.

**4.47** **Patch**: A program or software issued by a manufacturer to correct errors or vulnerabilities in software, an operating system, or other systems, in order to enhance stability and reduce vulnerability to attack by malicious actors.

**4.48** **Key Management**: The administration and management of keys used for the encryption and decryption of data, being a method of rendering data confidential and unreadable by any unrelated person.

---

## Chapter 2: Information Technology Security Policy

### Article 5: Policy Statement

The Information Technology Security Policy is hereby established in accordance with the Standards, Guidelines, and Procedures, to cover all aspects of the security of information systems in order to protect against various threats, with the following objectives:

5.1 To build confidence and ensure security in the use of the Company's and its affiliates' information systems or computer networks, so that operations may be carried out efficiently and effectively.

5.2 To define the scope of the administration of information system security by reference to the ISO/IEC 27001 standard, with continuous improvement.

5.3 To disseminate this Policy so that employees of the Company and its affiliates at every level are informed of it, and employees must comply with this Policy strictly.

5.4 To establish standards, guidelines, and procedures so that Executives, System Administrators, Employees, Contract Workers, Interns, and External Parties performing work for the Company are aware of the importance of maintaining security in the use of the Company's and its affiliates' information systems, and must comply strictly.

**Article 6: Policy Structure**

Section 1: Physical and Environmental Security

Section 2: Access Control Security

Section 3: Use of Computer and Mobile Device

Section 4: Use of the Internet and Online Social Networking

Section 5: Use of Electronic Mail

Section 6: Backup and IT Continuity Plan

Section 7: Removable Media Handling

Section 8: Security Awareness and Training

Section 9: Cyber Security

Section 10: Cloud Security

Section 11: Secure System Development Life Cycle

Section 12: Data Security

Section 13: Bring Your Own Device Policy

The components of each of the Sections referred to above shall consist of the objective, details of the standards, guidelines, and procedures for maintaining the security of the Company's information.

---

**Section 1: Physical and Environmental Security**

**1. Objective:**

To establish measures for controlling, preventing, and maintaining the security relating to entry into, or access to, buildings, premises, and information technology system workspaces, and further to establish measures for controlling, preventing, and maintaining the security of workspaces in which personal data is collected, used, or processed, having regard to measures appropriate to the importance of the information systems and data concerned, which constitute valuable assets that may need to be kept confidential.

**2. Designation of Areas Requiring Security**

2.1 The location of information systems shall be designated as a controlled-access area, and access shall be permitted only to those who have been granted rights and who have a genuine need to enter.

2.2 Information technology system workspaces shall be appropriately classified and designated for the purpose of monitoring and controlling the security of information systems against unauthorized persons, and to prevent other damage that may occur.

2.3 Information technology system workspaces shall be clearly designated and demarcated, and a floor plan showing the location of such workspaces shall be prepared and announced for general awareness.

2.4 System Administrators shall be granted rights of access to information technology system workspaces in order to perform the duties assigned to them in full, comprising the following:

2.4.1 Preparation of a register of persons entitled to enter and exit the area for the purpose of using information systems;

2.4.2 Recording of entry into and exit from the workspace, and designation of the person responsible for maintaining such records, by preparing documents or data recording entry and exit from the area;

2.4.3 Daily review of the history of entry into and exit from information technology system workspaces, and updating of the list of persons entitled to enter and exit the area at least once a year;

2.5 The IT Department reserves the right to suspend access to information technology system workspaces if a breach of information security is found, or if a threat that may cause damage to the Company is detected.

---

**Section 2: Access Control Security**

**1. Objective:**

To establish measures controlling access to the Company's information systems by unauthorized persons, and to prevent intrusion via network systems by intruders using malicious code, which could damage information systems or cause information systems to cease functioning, and to enable the verification and tracking of the identity of persons accessing the Company's information systems accurately.

**2. Control of Access to Information Systems**

2.1 System Administrators are responsible for verifying approvals, and for granting and amending users' rights of access to information systems, and shall document the granting of system access rights, and shall retain such documentation as evidence.

2.2 The Data Owner Department or System Owner Department shall permit users to access information systems, or shall grant rights, only to the extent necessary for the performance of their duties, in order to prevent the granting of access rights in excess of what is necessary, which could give rise to a risk of use beyond one's authority.

2.3 System Administrators shall grant access rights to information systems on the principle of least privilege, so that users may perform only the duties assigned to them.

2.4 There shall be a segregation of duties between System Administrators who access the database and those who access the operating system, as appropriate, so that no System Administrator is able to carry out the entire information system management process from beginning to end.

2.5 System Administrators shall establish a method for terminating connections to information systems following a period of inactivity (Session Time-out), as specified in Procedure "P-(G-HC-IT)-002, Information System Service Standard."

2.6 Two-Factor Authentication

2.6.1 System Administrators shall provide two-factor authentication for access to important information systems;

2.6.2 Users shall register their personal mobile device in order to use two-factor authentication as provided by the Company;

2.6.3 The use of two-factor authentication devices shall require approval from the IT Department;

2.6.4 In the event that a mobile communication device or token is lost, or there is suspicion that a password has been compromised, the user shall immediately notify the IT Department;

**3. Management of User Accounts and Passwords**

3.1 The registration of new users shall be governed by formal procedures, so as to grant rights necessary for use, including procedures for the revocation of access rights, such as upon resignation or a change of position within the Company.

3.2 The Company does not permit the use of Shared User Accounts.

3.3 Where it is necessary to grant a user special or maximum privileges, the control of such privileged users shall be carefully considered, having regard to the following factors:

3.3.1 Approval must be obtained from the Manager of the IT Department, or a person assigned by the Manager of the IT Department, together with the relevant System Administrator;

3.3.2 Strict controls on use must be in place, such as restricting use to cases of necessity only;

3.3.3 A period of use must be specified, and use must be suspended immediately upon the expiry of that period;

3.3.4 The password must be changed strictly every time such special access is no longer required;

3.4 Use of Passwords

3.4.1 A user who receives a password for the first time must change it immediately so that it becomes confidential to that user alone; where a password has been disclosed, or there is suspicion that another person has learned a user's personal password, the user must change the password immediately;

3.4.2 Guidelines for password management shall follow Procedure "P-(G-HC-IT)-002, Information System Service Standard," and must be strictly complied with;

**4. Management of Network Access**

4.1 The person responsible for overseeing the communication network, and for determining, amending, or changing system configuration values, shall be clearly designated.

4.2 System Administrators shall design the network system according to the groups of information system services in use, groups of users, and groups of information systems, such as an Internal Zone and an External Zone, so that control and prevention of intrusion may be carried out systematically.

4.3 System Administrators shall establish a method for restricting access rights, so as to control users so that they may use only the networks for which they have been authorized.

4.4 The System Administrator responsible for determining, amending, or changing the various parameters of the network system and of devices connected thereto shall be clearly designated, and such parameters shall be reviewed at least once a year; in addition, any determination, amendment, or change of parameters should be notified to relevant persons on every occasion.

4.5 All of the Company's network systems connected to other networks outside the Company should be connected via an intrusion-prevention device or packet-filtering program, such as a firewall or other hardware, and must also be capable of detecting malware.

4.6 An intrusion detection/prevention system (IPS/IDS) shall be installed to monitor unusual access to the Company's network by persons, and any amendment of the network system by unauthorized persons.

4.7 Access to the Company's internal network system via the internet shall require login and authentication in order to verify accuracy.

4.8 The IP addresses of the Company's internal network system must be protected from being visible to connected external units, in order to prevent outsiders from readily learning information about the structure of the network system and the components of the information systems.

4.9 A Network Diagram shall be prepared, containing details of the scope of the internal and external networks and of the various devices, and shall be kept up to date at all times.

4.10 The use of tools for inspecting the network system should be approved by the System Administrator, and their use restricted to what is necessary.

4.11 The installation and connection of network devices shall be carried out by System Administrators only.

**5. Server Management**

5.1 The person responsible for overseeing servers, and for determining, amending, or changing the various values of system software, shall be clearly designated.

5.2 There shall be steps or procedures for inspecting servers, and, where usage or a change of values in an abnormal manner is discovered, corrective action shall be taken, together with immediate reporting.

5.3 Only necessary services, such as SSH or SFTP, shall be enabled; where a necessary service carries a risk to the security system, additional protective measures shall be put in place.

5.4 System software, such as web server software, shall be regularly updated to remain current, in order to close vulnerabilities.

5.5 System software shall be tested for security and general operational efficiency prior to installation, and following any correction or maintenance.

5.6 The installation and connection of servers shall be carried out by System Administrators only.

5.7 Consideration shall be given to installing patches appropriate to network devices and network security devices, in accordance with manufacturers' recommendations, and such installation shall be carried out through the change management process in accordance with Procedure "P-(G-HC-IT)-006: Information System Management."

**6. Control of External Access to Information Systems**

6.1 Remote access to the Company's or its affiliates' computer network systems creates a channel that carries a high risk to the security of the Company's data and resources. Controlling users who access the Company's information systems remotely therefore requires the establishment of security measures more stringent than the standards applicable to internal access.

6.2 Any method by which remote access to information systems may be obtained shall require prior approval from the Manager of the Human Resources and Corporate Support Department, or a person assigned by that Manager, and shall be strictly controlled before use, and the user must strictly comply with the requirements governing system and data access.

6.3 Users must not give their User Account for remote access to information systems to any other person to use, and shall be responsible for any resulting damage.

6.4 The Company reserves the right to suspend remote access to information systems where there is reasonable cause to suspect that a computer is not safe for the network system.

6.5 When a user seeks to access information systems remotely, authentication shall be required in accordance with the method provided by the Company.

**7. Management of Logging and Audit**

7.1 System logs (of server operation), network logs, application logs, and security logs (of the intrusion-prevention system), which shall be deemed to include systems that collect or process personal data, shall be maintained, with online logs retained for 3 months and offline logs retained for 9 months, for audit purposes.

7.2 Log data arising from user accounts at every level (both Privileged Users and Non-Privileged Users) shall be retained.

7.3 System Administrators shall regularly review users' activity logs.

7.4 There shall be a method for preventing the alteration of logs, and access to such logs shall be restricted to relevant persons only.

7.5 Log data relating to access to the Event Logging Storage shall be retained.

7.6 A process for monitoring and reviewing event log data shall be established, together with an alert system for when events occur.

**8. Authorization for Temporary Personnel to Access Information Systems**

8.1 A department that needs to obtain approval for temporary personnel to access information systems shall proceed in accordance with Procedure "P-(G-HC-IT)-001, Process for Requesting Information Services" and Procedure "P-(G-HC-IT)-005, Process for Granting and Reviewing Information System Access Rights."

8.2 The head of the department shall control the use of information systems by temporary personnel in accordance with this Policy, and shall notify the System Administrator immediately once such temporary personnel no longer require access, or upon early termination of their engagement.

---

**Section 3: Use of Computer and Mobile Device**

**1. Objective:**

To ensure that users are aware of their duties and responsibilities in using the Company's computers and mobile devices; users must understand and strictly comply with this Policy, so that the Company's data and devices remain secure and continuously available, including with regard to maintenance and matters to be avoided, so as to achieve maximum efficiency in use.

**2. General Use**

2.1 Users are responsible for maintaining the security of their computer and preserving its condition so that it remains in its original state and continuously available for use, and must not modify or alter any component of the computer.

2.2 Computers and mobile devices that the Company permits users to use are the property of the Company; users must use them efficiently for the Company's business purposes only, must keep them in a safe place to prevent loss, and must not allow such devices to be used by any other person.

2.3 Users must not use the Company's computers, computer equipment, or other resources for personal business gain, for disseminating inappropriate information, or for any act contrary to law, morality, the nation, religion, or the Monarchy, or that endangers security or society.

2.4 Programs installed on the Company's computers are programs for which the Company has lawfully purchased a license; users are therefore prohibited from copying such programs and installing them on personal computers, or from modifying them, or from providing them to any other person for use unlawfully.

2.5 Users are prohibited from using unauthorized software with the Company's computers or mobile devices; and, if a claim is brought by an aggrieved party, the user shall be liable for the full amount of any resulting damage.

2.6 Users are prohibited from using computer equipment to produce, possess, or distribute computers or software that is inappropriate or unlawful.

2.7 Users shall be fully responsible for all text, images, sound, or files transmitted from their computer.

2.8 The naming of computers (Computer Name) shall be determined by the Company's System Administrator only.

2.9 The relocation or dispatch of computers for repair shall be carried out only by the IT Department or a person assigned by it.

2.10 Users should study and follow the user manual in detail, so as to use devices safely and efficiently.

2.11 Users should store the Company's important data in the manner provided by the Company, such as on SharePoint, OneDrive, or removable storage media provided by the Company.

2.12 Users must not store data on Drive C or on the Desktop.

2.13 Shortcuts or buttons linking to the Company's important data should not be created on the Desktop.

2.14 Users must report any abnormal event relating to a computer, computer equipment, computer data, or information to the System Administrator.

2.15 The Company reserves the right to inspect a computer where there is reasonable cause to suspect that a user has done anything that may cause damage to the Company.

2.16 Users must report the loss or theft of a mobile device to the IT Department as soon as the loss or theft becomes known.

**3. Control of Access to the Operating System**

3.1 Users should set passwords in accordance with Procedure "P-(G-HC-IT)-002, Information System Service Standard."

3.2 Users must lock their screen immediately whenever the computer is not in use, and must re-enter their password when they wish to resume use.

3.3 Users must log off immediately upon finishing use or when away from the screen.

**4. Protection against Computer Viruses and Malware**

4.1 System Administrators shall regularly update anti-virus software in order to close vulnerabilities arising from software and to protect against various threats.

4.2 System Administrators are responsible for installing anti-virus software on computers.

4.3 System Administrators or users must scan removable media for viruses every time before use with a computer.

4.4 Users must not adjust or disable the operation of anti-virus software installed on their computer by the System Administrator.

4.5 Users who take a computer outside the network must, upon reconnecting to the network, carry out a virus scan themselves, in accordance with the arrangements made by the System Administrator, on every occasion.

4.6 Users must not download data or software from inappropriate websites.

4.7 Users are responsible for immediately notifying the System Administrator, and are prohibited from connecting their computer to the network, if they suspect or discover that their computer is infected with a virus or malicious code, in order to prevent its spread to other computers.

4.8 Users must not connect computer equipment or mobile devices that do not belong to the Company to the network, except with prior approval.

4.9 Users should scan files attached to e-mails, or files downloaded from the internet, with anti-virus software before use.

4.10 The Company reserves the right to prevent a computer that is infected with a virus, or is suspected of carrying a virus, from connecting to the Company's internal network

---

**Section 4: Use of the Internet and Online Social Networking**

**1. Objective:**

To ensure that users are aware of the rules and guidelines for the safe use of the internet and online social networks, and to prevent violation of the Computer-Related Crime Act, such as by sending data, text, commands, sets of commands, or anything else within a computer system to another person, so as to disturb another person's peaceful use of a computer system, or to cause the Company's computer system to be suspended, delayed, obstructed, or disrupted so that it cannot function normally.

**2. Use of the Internet and Online Social Networking**

2.1 Users must not use the Company's internet for personal business gain or to access inappropriate websites, such as websites contrary to morality, websites whose content is contrary to the nation, religion, or the Monarchy, or websites that endanger society.

2.2 Users must not use the Company's internet to import, disseminate, or forward computer data that is false, that constitutes an offense relating to national security, that constitutes an offense relating to terrorism, or that contains obscene images.

2.3 Users must not import computer data consisting of an image of another person that has been created, edited, added to, or altered by electronic or other means in a manner that would damage that person's reputation, subject them to contempt or hatred, or cause them humiliation.

2.4 Users must not use online social networks in a manner that causes damage to the Company, infringes rights, causes annoyance to others, is unlawful, is contrary to morality, or seeks or permits another person to seek business benefit for personal gain.

2.5 In expressing opinions, users must not use provocative or defamatory language that would damage the Company's reputation or harm relationships with officials of other organizations.

2.6 Users are responsible for verifying the accuracy and reliability of computer data found on the internet before using it.

2.7 Users are prohibited from disclosing important confidential information relating to the Company's business, which has not yet been officially announced, via the internet.

2.8 Users shall be granted access to sources of information according to their duties and responsibilities, for the efficiency of the network and the security of the Company's data.

2.9 Users must not discuss or transmit confidential information via online social networks.

2.10 Users must not use their Company e-mail account to register for online social networks.

2.11 Users must exercise caution when downloading programs for use from the internet, including patches or fixes from vendors, and must do so without infringing intellectual property rights.

2.12 Users must not use the Company's internet to download music, games, hacking tools, or any program that may cause network congestion.

2.13 After finishing use of the internet, the web browser shall be closed, in order to prevent access by other people.

---

**Section 5: Use of Electronic Mail**

**1. Objective:**

To establish measures for the use of e-mail; users must give due importance to, and be aware of, problems that may arise from the use of e-mail services over the internet network. Users must understand the rules established by System Administrators, must not infringe any rights or do anything that would create problems or fail to respect the rules established, and must strictly follow the guidance of the System Administrator, so that the use of e-mail over the network system proceeds safely and efficiently.

**2. Use in Sending E-mail**

2.1 System Administrators shall grant e-mail system access rights appropriate to the services accessed by, and the duties and responsibilities of, each user, and shall continuously and regularly review such access rights.

2.2 System Administrators shall assign a new user account and password for a user's first use, for the purpose of verifying the authentic identity of the user of the Company's e-mail system.

2.3 Users should exercise caution in using e-mail, so as not to cause damage to the Company, infringe rights, cause annoyance to other persons, act unlawfully, or act contrary to morality, and must not seek, or permit others to seek, business benefit from the use of e-mail over the Company's network system.

2.4 Users must not use another person's e-mail address to read, receive, or send messages, except with the consent of, or delegation from, the owner, and the owner of an e-mail account shall be deemed responsible for all use of that account.

2.5 Users must use their Company e-mail address for the Company's business purposes only.

2.6 After finishing use of the e-mail system, users must log off every time, in order to prevent access by other persons.

2.7 Users accessing e-mail via Web Access must sign out every time after use, and must not save the account name and password on the computer.

2.8 Users must check e-mail attachments before opening them, by scanning the file with anti-virus software, in order to guard against opening executable files such as .exe or .com files.

2.9 Users must not open a file attached to an e-mail from an unknown sender unrelated to Company business, nor forward such an e-mail, unless it has been virus-checked.

2.10 Users should use polite language that is proper according to the customary practice for the use of e-mail.

2.11 Users must not use impolite language, or send or receive inappropriate e-mails, which may damage the Company's reputation or create discord within the Company through the use of e-mail.

2.12 Users should check their e-mailbox every day and should keep the number of files and e-mails they retain to a minimum.

2.13 Users must not send text, images, sound, or files to all users (All Group Mail), except for executives at department-manager level or above, or equivalent, or representatives of departments who have received approval from the responsible person, and the content sent must relate to the Company's business.

---

**Section 6: Backup and IT Continuity Plan**

**1. Objective:**

To provide guidelines for the backup of the Company's data and information systems, including testing to prepare for the recovery of information systems in the event of an emergency, and to ensure that data and information systems remain continuously available and efficient when needed.

**2. Backup of Data and Information Systems**

2.1 System Administrators shall back up important business data, including operating systems, application databases, and the commands used for operation, in full, so that they remain continuously available.

2.2 System Administrators shall prepare a data backup procedure to serve as an operating guideline.

2.3 System Administrators shall store backup data off-site, for security in the event that the primary data center is damaged, and such off-site location shall be subject to access controls and physical damage-prevention measures.

2.4 System Administrators shall prepare procedures for the destruction of important data and storage media that are no longer in use, including important data of various types, in accordance with the Company's data classification.

**3. Preparedness for System Recovery in the Event of an Emergency**

3.1 An information system recovery plan shall be prepared to support the continuity of the Company's business.

3.2 The information system recovery plan shall be kept up to date at all times, and shall be communicated to relevant persons.

3.3 The information system recovery plan shall be rehearsed at least once a year, in order to ensure that it can be applied in practice, and the results of such testing shall be recorded.

3.4 Users shall cooperate with the Company in rehearsing the information system recovery plan or any other plan relating to the maintenance of information system security.

---

**Section 7: Removable Media Handling**

**1. Objective**

To establish guidelines for preventing the unauthorized disclosure, alteration, removal, or destruction of information systems stored on removable media, or their unintentional leakage, and further to reduce the risk of the spread of malware or the use of such media as a channel of attack by malicious actors.

**2. General Use**

2.1 Users must use only removable media provided by the Company that is capable of data encryption and has been registered with the Company, and must not connect the Company's removable media to a computer that is not registered with the Company or has not been security-checked by the IT Department.

2.2 Users are responsible for ensuring that the Company's removable media remains secure and continuously available for use.

2.3 When removable media is no longer required, the user must erase the data and return the removable media to the IT Department.

2.4 Removable media shall be registered so that it can be tracked and the risk of data leakage reduced.

**3. Disposal of Removable Media**

For removable media that is no longer in use, the IT Department shall carry out the destruction of the data on such removable media.

**4. Reporting of Loss**

Users must immediately report the loss of removable media to the IT Department.

---

**Section 8: Security Awareness and Training**

**1. Objective:**

To establish guidelines for building information security awareness and providing training to users efficiently and with earnest implementation; users must strictly comply, to reduce the risk of creating vulnerabilities that malicious actors could exploit to launch attacks and cyber threats.

**2. Building Awareness and Training**

2.1 The Responsible Department shall prepare and review an information security awareness strategy for users within the Company.

2.2 The Responsible Department shall develop and improve information security awareness curricula to keep them appropriate to current circumstances.

2.3 The Responsible Department shall organize training sessions to build information security awareness, and shall communicate this Regulation to users, together with establishing criteria for measuring effectiveness on a regular basis.

2.4 The Responsible Department shall report the effectiveness of its information security awareness activities to Executives.

2.5 Users must regularly attend training and undergo testing on information security awareness.

2.6 Where a user fails to pass an information security awareness test in accordance with the specified criteria, the Responsible Department shall report the test results to the user's home department, and reserves the right to temporarily suspend that user's access to information systems until the specified criteria are met.

2.7 The Responsible Department shall arrange PDPA Awareness Training on the Personal Data Protection Act B.E. 2562 (2019) for all Company employees, so as to provide knowledge of information security relating to personal data and to ensure that employees comply with the personal data protection law, as well as with the Company's related policies and operating procedures for personal data protection; such training shall be provided to new employees before they commence work and to all employees annually, and the Company shall keep records of such training as evidence.

---

**Section 9: Cyber Security**

**1. Objective:**

To provide guidelines for the effective management of cyber security, efficient risk management, and the prevention of cyber threats that may cause damage to information systems and continuously affect the Company's business operations.

**2. Management of Cyber Security**

2.1 The Responsible Department shall regularly report cyber security incidents to Executives.

2.2 Control measures and risk management for cyber security shall be established to reduce risk and prevent cyber threats.

2.3 There shall be prevention, monitoring, intrusion detection, and response to cyber threats, together with regular reporting of the results of such monitoring to Executives.

2.4 A vulnerability assessment of information systems shall be conducted at least twice a year, or whenever a significant change is made to an information system.

2.5 A penetration test shall be conducted, for information systems at risk from cyber threats, at least once a year, or whenever a significant change is made to an information system.

2.6 The Responsible Department shall prepare a cyber threat response plan, including conducting a rehearsal of the plan at least once a year and assessing its effectiveness in order to improve the next rehearsal.

2.7 Every department involved in rehearsing the cyber threat response plan shall provide cooperation, support, and encouragement so that it is implemented in earnest.

---

**Section 10: Cloud Security**

**1. Objective:**

To provide guidelines for the use of cloud services, both from within the Company and from external providers, in a secure manner that does not affect the Company's information systems.

**2. Use of External Cloud Services**

2.1 The Responsible Department shall prepare a procedure for managing external cloud service providers in accordance with information technology security principles.

2.2 In using external cloud services, the Responsible Department shall select a provider certified to a cloud security standard, such as the Cloud Security Alliance or ISO/IEC 27017.

2.3 The Responsible Department shall arrange for the assessment and selection of external cloud service providers.

2.4 The Responsible Department shall have a Service Level Agreement covering information security and personal data.

2.5 The Responsible Department shall regularly monitor and review the operation of the cloud system.

2.6 The Responsible Department shall assess the service of the external cloud service provider at least once a year.

2.7 The Responsible Department shall report information security incidents affecting business operations to Executives.

2.8 The Responsible Department shall regularly assess information security risk relating to the cloud system.

2.9 Information systems installed on the cloud system shall appropriately encrypt data received and transmitted over public networks.

2.10 Where a transfer is made to another external cloud service provider, the copying or transfer of data (Data Portability) between cloud systems shall be carried out securely.

2.11 Upon termination of an external cloud service, the Responsible Department shall instruct the external cloud service provider to destroy or delete the Company's data held on the cloud system.

---

**Section 11: Secure System Development Life Cycle**

**1. Objective:**

To ensure that the development of the Company's information systems is consistent with users' needs and follows a development approach consistent with generally accepted international information security standards.

**2. Design and Development of Information Systems**

2.1 The Responsible Department shall develop or improve information systems in accordance with international standards.

2.2 The Responsible Department shall establish a secure information system development procedure, covering information security and personal data.

2.3 System Administrators shall separate the Production Environment from the Test Environment and the Development Environment.

2.4 Where the development of an information system involves the transmission of data over a public network, the Responsible Department shall assess the risk of transmitting and transferring such data and shall put in place appropriate security control measures.

2.5 The Responsible Department shall prepare operating manuals and documentation relating to the information system being developed, and shall keep them up to date.

**3. Protection of Test Data and Testing of Information Systems Prior to Go-Live**

3.1 Persons involved in developing an information system shall participate in testing, to ensure that the information system developed or amended operates efficiently, meets requirements, and is secure.

3.2 System developers shall protect the data or information used for testing an information system, and shall control the use of such data or information so that it remains secure and data leakage is prevented.

3.3 The Responsible Department shall arrange for security testing of an information system prior to its going into live service.

**4. Control of Access to the Development Environment and Source Code**

4.1 Where an external party is engaged to develop an information system, the Responsible Department shall grant access only to the Development Environment.

4.2 System Administrators shall provide a repository for storing source code and shall grant access rights only to authorized persons.

4.3 System Administrators shall maintain log data of access to, and changes made to, source code.

---

**Section 12: Data Security**

**1. Objective**

To establish control measures for the management of data security within information systems, consistent with the principles of confidentiality, integrity, and availability, and to reduce risks that may cause damage to the Company's business operations.

**2. Management of Data Access**

2.1 Users must identify the confidentiality classification of data and encrypt it appropriately to prevent disclosure or leakage, such as by using 7-Zip password protection.

2.2 Data held in application systems and on storage media (Data at Rest) shall be designed and managed to ensure that it is stored securely, with appropriate access rights, and shall be encrypted in accordance with an industry-accepted standard, such as Advanced Encryption Standard 256 (AES256).

2.3 System Administrators shall prepare an Encryption Data Matrix, specifying the type of data, its storage location, control and protection measures, and the retention period of the data.

2.4 System Administrators shall document Key Management details, specifying the key generation process, the key retention period, and the key protection procedure, to support data encryption.

2.5 System Administrators shall grant data access rights only to persons who have such rights and have been authorized by the Data Owner Department.

2.6 Information systems and databases shall be configured with separate user accounts and access rights appropriate to job function.

2.7 System Administrators shall implement Data Loss Prevention measures to prevent unauthorized sharing of Company data.

2.8 The Data Owner Department shall notify System Administrators to store the Company's data and information in accordance with legal requirements.

2.9 System Administrators shall establish procedures for monitoring and maintaining logs of data access and of the Company's information systems.

**3. Exchange of Data**

3.1 Where it is necessary to exchange Company data with an external party, approval from Executives shall be obtained, and the Responsible Department shall assess the risk, establish control measures, and provide a secure method of data exchange.

3.2 The receipt and transmission of high-risk or confidential data over a public network shall use secure technology, such as SSL using TLS Protocol version 1.2 or higher, and shall employ an industry-accepted advanced encryption standard, such as Advanced Encryption Standard 256 (AES 256).

3.3 Users must not share, store, or send Company data via a public platform to unauthorize persons.

3.4 Users may share, store, and send data only via platforms authorized by the Company, such as Microsoft Teams, SharePoint, or OneDrive.

**4. Backup and Destruction of Data**

4.1 System Administrators shall establish procedures for backing up and recovering data stored on servers, and shall regularly perform data backups.

4.2 System Administrators shall establish effective procedures for the destruction of data and storage media, to prevent leakage of the Company's data.

4.3 System Administrators shall maintain records evidencing the destruction of data and storage media, for retention as evidence for audit purposes.

**5. Oversight of External Parties**

For the procurement, development, and maintenance of information systems relating to personal data that must be carried out by, or jointly with, an external party, the Company shall arrange for an assessment of such external party in respect of personal data protection, in accordance with the Guideline for Third Party Assessment - Data Privacy Protection.

---

**Section 13: Bring Your Own Device Policy**

**1. Objective:**

To establish measures for the use of personal mobile devices, or their connection to the information systems of the Company and its affiliates, to proceed smoothly and securely, without affecting the operation of the Company's information systems and data.

**2. Requesting Access to Information Systems**

2.1 In order to access the Company's information systems or information data, a user must register their personal mobile device and install Enterprise Mobile Management (EMM) software.

2.2 The IT Department shall review the personal mobile device operating system standards set out in Procedure "P-(G-HC-IT)-002, Information System Service Standard," at least once a year.

2.3 Users must update the operating system of their personal mobile device in accordance with the standards set by the Company in Procedure "P-(G-HC-IT)-002, Information System Service Standard."

2.4 Where confidential Company data is stored on a personal mobile device, the user must comply with the confidentiality classification and security requirements applicable to the Company's documents, and such data must be encrypted to prevent leakage.

**3. Responsibility for Personal Mobile Devices Containing the Company's Information**

3.1 In the Event of Loss or Theft

3.1.1 Users must report the loss or theft of a personal mobile device to the IT Department as soon as the loss or theft becomes known, so that the Company's information may be erased before the matter is reported to the telecommunications network provider;

3.1.2 The Company has the right to erase its information from a personal mobile device in the event of loss or theft;

3.1.3 In the event of the discontinuation or replacement of a personal mobile device, the user must report such discontinuation or replacement to the IT Department in advance;

3.2 Users may download and install applications only from standard application stores, such as the Apple Store and Play Store.

3.3 Users are responsible for backing up all of their personal data. The Company shall not be liable for any damage arising from the deletion of data and applications on a personal mobile device, where the Company considers such action necessary to protect the Company's information, even if data is inadvertently deleted as a result.

3.4 Management of the Functions of Personal Mobile Devices

3.4.1 Users must delete, or notify the IT Department to delete, the Company's information from a personal mobile device before transferring the device to any other person by any means;

3.4.2 The Company does not permit devices that have been jailbroken or rooted, or whose security system has otherwise been modified, to be used;

3.4.3 Users must exercise caution in allowing other persons to use their personal mobile device, and are responsible for any act carried out under the user's identity, and must not disclose their password or other personal data to any other person;

3.5 Security of Personal Mobile Devices and Information

3.5.1 Users must exercise caution in allowing other persons to use their personal mobile device, and are responsible for any act carried out under the user's identity, and must not disclose their password or other personal data to any other person;

3.5.2 Users must keep their personal mobile device continuously updated to the Company's standards, as set out in Procedure "P-(G-HC-IT)-002, Information System Service Standard";

3.5.3 Users must set a password or other authentication method before using their personal mobile device;

3.5.4 Users must configure automatic screen lock (Display Auto Lock on iOS, Screen Timeout on Android) to activate after no more than 5 minutes of inactivity;

3.5.5 Users must not leave a personal mobile device where it can easily be seen, even for a short period, and must not leave a mobile communication device in a vehicle overnight;

3.5.6 When using a personal mobile device to display confidential information of the Company or its affiliates in a public area, such as on a train, an airplane, or in a coffee shop, the user must position the device so that others cannot see the screen, in order to protect the information of the Company and its affiliates, or must dim the screen or use a privacy screen filter to reduce or prevent visibility of the screen from certain angles;

**4. Technical Support and Conditions for Assistance**

4.1 Service Desk staff shall provide technical support for personal mobile devices authorized to connect to the Company's network system, information systems, or applications used for work, and only in relation to matters concerning work performed for the Company.

4.2 Service Desk staff shall not help with the provision of replacement devices, device upgrades, use of personal mobile devices generally, or use of other applications unrelated to work performed for the Company.

4.3 Service Desk staff shall assist only with the Company's applications and with loading the Company's information onto a personal mobile device; for any other matter, the user must contact the network service provider or the retail store where the device was purchased directly.

**5. Access to Personal Data**

The Company shall not access the personal data of a user from the user's personal mobile device, nor disclose such data to any third party, except with the user's written consent, or unless the Company receives a written request from a relevant government authority.

**6. Termination of Employment**

6.1 Upon termination of a user's employment, the Company shall erase all Company's and its affiliates' information from the user's personal mobile device.

6.2 A user whose employment has ended shall have no right to recover the Company's or company affiliates' information, or any applications arising during their employment with the Company; any attempt to recover any of the Company's data shall be deemed a wrongful act on the part of the user.

---

**Chapter 3: Policy Compliance and Review**

**Article 7** Compliance with this Policy shall be audited, and the results shall be reported in accordance with the internal audit procedures under the principles of the Information Technology Security Management System standard.

**Article 8** The IT Department shall be responsible for proposing the review or improvement of this Policy and its requirements on an annual basis, and the results of the internal audits referred to above shall be considered as part of that review.

**Article 9** A user who violates or fails to comply with this Policy, including the criteria and guidelines for maintaining the security of information systems issued under this Policy, shall be deemed to have committed a disciplinary offense and shall be liable for any resulting damage to the Company or to any other person.

This Regulation shall come into force as of October 1, B.E. 2565 (2022).

**Announced:** October 12, 2022
**Managing Director:** (Mr. Pairoj Samutthananon)