Information Technology and Cyber Security Policy

Introduction

The Company focuses on creating value of products and services to be appropriated with customer requirements for each area together with cost management and operating expenses to be at the proper level so that the company can deliver the highest worthiness of goods and services to customers. In order to achieve it visions to be the best distribution channel for building materials and home furnishings of ASEAN. Beside of management subject to good governance principle and focusing on excellent work procedure, the Company also aims to develop distribution channels, build customer relationships, work collaboratively with business partners, together with improve the Information technology system and human resource development to support the growth and create value added properly to stakeholders and collective society. Thus, the Company has established the Information Technology and Cyber Security Policy to control and support the security management of Information Technology to build confidence in operating activities of the Company and to be legally applicable.

All Information Technology systems of the Company are operating on a 100% Cloud-based system, including security measures such as Back up, Recovery, and Business Continuity Planning (BCP). The Cloud system can help reduce the necessity of using hardware systems, minimize electricity consumption and energy resources, and cut down expenses on hardware maintenance and system upkeep. Additionally, the Cloud system can also contribute to reducing manpower requirements, saving time in network management and maintenance. The use of Cloud Servers helps decrease the workload related to system administration and management. Cloud services are equipped with user-friendly web-based control panels, enabling system administrators to easily monitor and control Cloud Servers through a straightforward interface. Furthermore, detailed event tracking and logging are available for Cloud Servers over an extended period, facilitating swift examination and future actions.

Objectives

1. To stipulate the principle and regulation in management of Information Technology Security.
2. To build knowledge to employees to correctly comply with the policy including laws related with Information Technology.
3. To prevent the Information Technology system from interruptions and cyber-attacks in any forms this may cause damages to the business operations of the Company.

Policy Composition

1. **Accountability, Identification and Authentication**
   - 1.1 Authentication is the process of verifying identity of a user to access the system.
   - 1.2 Authorization is specifying user rights/privileges to resources for which menus they can use / or what they can do with the system.

1.3 Accountability is recording details of the application's use by the authentication of a user to access by the Company as follow;

1) Use the Fingerprint or Face Recognition for identification
2) Use OTP / Email to confirm the transaction.
3) Specify Secret Key / Token to Access the system (only the person who has Secret Key / Toke can access to the system, not include User / Password)

2. Assets Management

2.1 Users of the company's computers and computer devices must be responsible for the active asset.

2.2 Do not use the company's computers and computer networks in an inappropriate way. Do not allow users to install and modify software changes on a computer of the Company.

2.3 Unless authorized by the highest authority person of the authority responsible.

2.4 Computer equipment must not be stored or used in places of high heat, high humidity, dust and be aware of fall.

2.5 Avoid using solids to press against computer screens, which can cause scratches or cracks.

2.6 Moving computer equipment must be done with caution. Do not put heavy stuff over it or throw it.

2.7 Do not modify computer components and peripherals. If necessary, please notify the supervisor and users must maintain the intact condition of the computer and equipment.

2.8 Retired users must return all responsible computers and equipment to the responsible authorities in the conditions that are available to use and intact.

2.9 The user is responsible for preventing loss.

2.10 Do not install illegal or unrelated software to the work.

3. Data access control and Use of Information System

3.1 Specify the criteria for allowing access to information use in relation to authorization, specifying the rights or delegation of authority as follow;

1) Authorize or specify the rights of users for each involved group such as:
   - Read Only
   - Create Data
   - Revise Data
   - Approve
   - Cancel
   - Delete
2) Specify the criteria for suspension of right/authority in accordance with the user's access management as prescribed.

3) Users who require accessing the department's information system must be authorized by the executives.

3.2 Operational Procedures for data storage

1) Categorizing data into

- Administrative information such as Policy data, employee data, financial data

2) Prioritizing data that is

- High Priority Data
- Medium Priority Data
- Low Priority Data

3) Access level

- Executives Level
- General Users Level
- System Administrator or Authorized user level

4) Determining Access time

5) Determining Access channel

3.3 User Access Management

1) Determining user registration procedure covered the following stages:

- Create an information system request form for the user to fill in the form in order to:
- Check eligibility and follow the user registration process.
- Specify name, last name of users.
- Specify job position and department.
- Signature of user's supervisor is required.
- Checking and assigning appropriate access rights to the duty and responsibility.
- Information system access data and records are recorded and stored.
- There are criteria for authorization to access the information systems and elimination from the user's register in case of resignation, job rotation, transfer, relocation or termination, etc.

2) Review of User Access Rights, there must be process of reviewing access rights of information system users and updating user accounts at least once a year or when changes are made, such as resignations, job rotation, transfer and relocation, etc.

3.4 Data access Management subject to confidentiality classification,

1) System Administrators must define confidentiality levels. Data storage practices and practices for controlling data access to each confidentiality levels, both directly access and access through the information system.

2) Data Subject must review the propriety of data access right of users at least once a year to ensure that the assigned rights are always appropriated.
3) The practice of controlling data access of each confidentiality levels, both directly access and access through the information system. The System Administrator must define a user name and password to verify the identity of data user for each confidentiality levels.
4) Data transmission over public networks must be encrypted with international standards such as SSL, VPN or Encryption in any forms, etc.
5) Data security measures should be taken in case of computer maintenance or bring Computers out of the area, such as send the computer for repair, should back up and delete data stored in the media first, etc.

4. Backup Policy

4.1 Make copies of data and software stored in descending order of necessity of Information technology information backup to be arranged from high to low.
4.2 There are procedures for correctly preparing data backup and recovery both software systems and data in information technology systems that are separated by each information technology system.
4.3 Store the backed-up information in the storage media by typing the name on the storage media so that it can clearly represent the software system, date, backup time, and the responsible person for data backup. The backup data should be stored in a backup storage location installed at another location and requires testing of storage media, regularly backup.
4.4 Contingency plans must be drawn up to be able to recover the system within a reasonable period of time.

5. Network and Server Policy

5.1 System Administrators must divide the network by group of information services, user groups such as Internal Zone, External Zone, etc. in order to systematically control and prevent the cyber-attacks.
5.2 Connection of computers and devices to the company's computers and network system by users need to strictly obtain permission from the system administrator.
5.3 Do not act on the move, install, add, or do anything to the centralized devices such as Router, Switch, devices connected with the main network system without permission from the System Administrator.
5.4 Restriction method on use of right is required in order to control users to use only permitted network system. There must be restriction method on access way to the shared Network.
5.5 All networking system that are connected to other external network system, the department should connect through an anti-intrusion device, as well as must have the ability to detect malware.

5.6 Internal IP address of the internal network system of the department requires the protection from being visible of connected external entities.

5.7 A network diagram with details of the scope of internal and external networks and devices must be prepared as well as keep always up to date.

5.8 Log data should be stored in a storage media that can maintain the completeness, accuracy and identification of the person, who accesses it, and the information used in storage must define confidentiality levels in data access and system administrators are not allowed to edit the retained information except the IT auditor of the organization or the person assigned.

5.9 The user's application logs and details of the Intrusion Prevention System should be recorded, such as entry and exit log, user login attempt, Command Line and Firewall Log, etc. For the sake of monitoring and keeping such records for at least 90 days from the service ends.

5.10 The operating records of system users should be checked regularly.

5.11 There is strong control over the port used to access the system.

6. Internet and E-mail Security Policy

6.1 Setting a secure password

1) Password should be at least 8 characters long. Password should consist of lowercase and uppercase letters, numbers and symbols for more secure.
2) Avoid using your birth date, your name, as well as using other names that can be associated with you.
3) Dictionary words should not be used in your password whether single words such as home, or mix several words together such as Good Home. Due to hackers can use password cracking by comparing them from dictionary attack.
4) Use different passwords for different accounts, especially a password that uses access to important information, you may use the same password group, but change the numbers to separate it.
5) Do not replace some letters by similar-looking numbers, such as set password “H0use” by replacing the letter “O” with the number 0 (zero), the general person can guess even it's mixed.

6.2 Choose a secure Web browser

Browser selection should require protection against pop-ups, viruses, and data threats. In addition, it should be able to delete personal data, so you can be confident when you're browsing the internet while you're online.

6.3 Check to make sure your Internet connection is secure.

1) Always change your password (and user name) when you start your devices, you should not use the default value from the manufacturer.

2) Use WPA2 encryption for Data Theft Protection
3) The default SSID set by the manufacturer should not be used, as that Wi-Fi Router may be assessed as lack security protections, making it a target for attacks by hackers.
4) Enable MAC Address Filtering to ensure that only our devices are connected.
5) Disable SSID broadcast to keep your network safe from unauthorized access.
6) Disable automatic connections to public Wi-Fi networks which has risk of data leakage to external source.
7) Turn on the Firewall feature and install antivirus software to protect your devices on a Wi-Fi system.
8) Set up Static IP for devices in your home to tighten scope of use and security.

6.4 Regularly install an antivirus program and update virus database.

1) Install an antivirus program
2) Update Virus Database
3) Always scan virus before opening files from discs or storage media.
4) Beware of the threats by opening files from various storage media such as CD disk, flash drive, etc.
5) Always run a virus scan on your storage media before use.
6) Do not open files with strange, unknown or suspicious extensions, such as .pif. etc.
7) Do not use storage media from unknown sources.
8) Use caution when opening e-mails.
9) Do not open the e-mail files if the source is unknown.
10) Delete e-mail immediately if the source is unknown or has a strange file extension attached.
11) Be careful downloading files from the Internet.
12) Do not open unknown files attachment by chat programs such as Line, we chat, Facebook, twister, etc.
13) Do not open recommended websites via e-mail from unknown sources.
14) Do not download files from untrusted websites.
15) Keep track of virus attack alerts regularly.

7. Cryptographic Control

7.1 Data storage requires encryption of important data before storage, such as SHA-256 encryption.

7.2 Data retrieval requires that data access or retrieval must be retrieved through an API where a token is entered.

7.3 Connecting data to an Internet network requires encryption with SSL (Secure Socket Layer),

TLS (Transport Layer Security) technologies.

8. Physical and Environmental Security

8.1 Location-based Access Control

8.1.1 Allow entry and exit to the storage facility, IT Equipment installation area.

8.1.2 Assign rights to entry and exit to the storage facility, IT Equipment installation area.

8.1.3 Clearly workplace segregation.

8.1.4 Review the measure of entry and exit the storage facility, IT Equipment installation area.

8.2 Provide protection against damages caused by accidents or natural disasters.

8.2.1 Fire Protection System

- Fire extinguisher contain extinguishing agent.
- Fire extinguishing agents
- Smoke Detector
- Automatic injector for a gas fire extinguisher.

8.2.2 Flood Protection System

- Build a high-altitude building or computer laboratory.

8.2.3 Electrical power system protection system

- Install uninterruptible power supply (UPS) and automatic voltage regulator to prevent possible damages on the computer device or the processing of the computer system.
- Install generators for use in case of prolonged power outages that the company cannot operate and affect to workers and customers.

9. The Customer Data Privacy Protection Policy

9.1 The collection, use, disclosure of personal data requires the consent from the data subject.

9.2 Collect data from data subject as much as necessary.

9.3 Always keep personal data accurate and up-to-date.

9.4 Use personal data pursuant to the purpose requested, and if transmit data to others must first obtain permission from the data subject.

9.5 Define the data retention period pursuant to the purpose of use.

9.6 There are measures to keep personal data secure, such as encrypting sensitive data.

9.7 There is channel for the data subject to request the deletion of the stored personal data.

9.8 Appointment of Data Protection Officers (DPO)

Requesting Consent from customer through the storefront

Requesting Consent from customer through online channels

10. System Development

10.1 Coding is writing a set of computer programming instructions to perform specified tasks by using computer programming languages such as C++, C#, PHP, Java, Python, Dart.

10.2 Test is testing the program that the working process is correctly as required or not.

10.3 Deploy is the process to publish the correctly functioning programs goes up to sandbox / production for actual use.

10.4 Front-End is the part for user Interface that user can see and use.

10.5 Backup is Backup data to prevent data damages due to uncontrollable factors, such as Crashed HDD / Deleting data from malicious users, by the Company has done a Backup dividing to

- Daily Backup (after closing the system)
- Yearly Backup (Annually, at the end of the year)

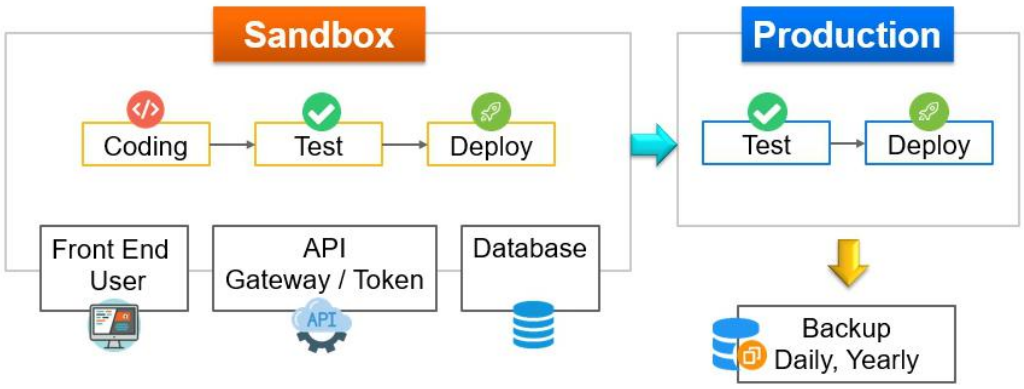
10.6 System Development and Testing Regulations

The Company has established sandbox (System Development and Testing Simulation Area) consist of

- -Server API Gateway
- -Database Server

10.7 Define that all development teams can develop programs only on sandbox.

System Development Flow



11. Cloud Usage and Cloud Security

11.1 Authentication and Security Auditing:

- Use an authentication system; users access the cloud only authorized persons.
- Regular security checks, monitor activity happening in the cloud, check for any potential problems.

11.2 Rights Management and Data Access

- Define data access rights to each level of user in the cloud.
- Data Encryption to protect data stored in the cloud and uses encryption for communication between the cloud and the user.

11.3 Risk Management and Monitoring

- Consistently assess and manage cloud-related risks.
- Intrusion detection systems risk management plan to investigate attacks and anomalies in the cloud.

11.4 Compliance with safety principles

- Constantly updating and securing the cloud.
- Improve and upgrade operating systems and software running in the cloud.
- Create a backup plan to ensure that important data stored in the cloud is not lost.

11.5 Training and Responsibility

- Training for users on security in the cloud.
- Clearly define the roles and responsibilities of cloud-related personnel.

12. The nature of cyber-crimes within the organization

12.1 Using passwords or impersonating others or their one-time passwords (OTP) to access the company's computer systems, reading, copying, approving, modifying, changing, or deleting information for personal gain or the gain of others through manipulation or deception. Using passwords or other users' credentials, one-time passwords (OTP), or intentionally providing others with passwords or user credentials, or intentionally allowing others to use their own passwords or user credentials and access rights to their computer systems.

12.2 Disclosing confidential business information or knowledge of the company to others without authorization from the company, with the intention of stealing or using the company's information to disclose, sell, or distribute to others for personal gain, resulting in harm to the company.

12.3 Covertly tampering with passwords or personal information of other users with the deliberate intention of unauthorized access to computer systems in order to engage in fraudulent activities against the company's assets or customers, or to tarnish the company's reputation.

12.4 Engaging in unauthorized copying or possession of materials that are inappropriate or illegal, such as offensive text, explicit images, or any other content that insults national institutions, religion, and the monarchy, or instigates division among the public or employees, or causes harm to the company.

12.5 Theft, smuggling, eavesdropping, routing, or decrypting electronic data using tools or other technologies to obtain unauthorized access to personal or confidential information of individuals or companies with the intention of causing harm to individuals or the company.

12.6 Intentionally and negligently causing harm to others by allowing unauthorized individuals to secretly or unlawfully access, disclose, distribute, or manipulate company data, attempting to gain unauthorized access to systems, or intentionally disrupting or damaging information, computer systems, or devices, thereby causing harm to the company.

12.7 Installing or using hacking tools or any other software related to the unauthorized access and retrieval of sensitive company data, except for individuals or departments responsible for information technology security.

12.8 Connecting computer devices or other electronic devices to the company's computer system or network without permission from the responsible department for configuration and installation, or modifying or changing IP addresses without authorization from the responsible department, altering, modifying, or relocating components of the computer system without permission, or adding additional components that do not belong to the company's assets without authorization.

12.9 Sending inappropriate messages or data using the company's email system or using the company's communication tools, such as insulting, harassing, threatening, defaming, or sending chain letters, using the internet, intranet, or email for matters unrelated to the company's business, using company-owned computers and other devices for personal entertainment or personal benefit.

12.10 Using unauthorized software that is not properly licensed according to the law or that the company has not authorized for use, or using software that may cause harm to the company.

12.11 Providing assistance or collaborating with external individuals to gain unauthorized access to the company's computer systems or information systems, engaging in activities of copying or destroying information or the company's computer systems.

13. Penalties for cyber misconduct within the organization

- Verbal warning
- Written warning
- Temporary suspension from work without pay.
- Dismissal
- Lay Off
- Criminal or civil proceedings

In the case of disciplinary action against an employee, the company is not necessarily required to follow the aforementioned sequence. The company may choose to impose penalties based on the severity of the misconduct committed. In addition, the Company will take the Information security/cybersecurity to be in part of the employee performance evaluation.

14. Cyber Security Measures and Incident Response

In addition to the aforementioned measures, employees of the company can report abnormal incidents and notify damages resulting from any cyber security through the IT Service Center, which may occur during their work. They can report via email to cybersecurity@globalhouse.co.th. There will be IT officer members responsible for handling reported incidents following the designed incident report and escalation process as quickly as possible. Communication and reporting will be directed to relevant stakeholders, including operation officer and relevant senior management. Additionally, there will be continuous follow-up until the issues are resolved.

Breaches Report

	2022
Total number of information security breaches	0
Total number of clients, customers and employees affected by the breaches	0

Modified and be effective from June 6th, 2023 onwards,

(Mr.Witoon Suriyawanakul)
Chief Executive Officer
Siam Global House Public Company Limited