Information Technology and Cyber Security Policy

Introduction

The Company focuses on creating value in products and services that align with customer requirements for each area, while managing costs and operating expenses to maintain an appropriate level. This ensures the Company can deliver the highest value in goods and services to its customers. To achieve its vision of becoming the best distribution channel for building materials and home furnishings in ASEAN, the Company emphasizes management based on good governance principles and excellent work procedures. Additionally, the Company aims to develop distribution channels, build customer relationships, collaborate with business partners, and improve the information technology system and human resource development. These efforts support growth and create added value for stakeholders and society as a whole. Therefore, the Company has established the Information Technology and Cyber Security Policy to control and support the security management of information technology, building confidence in the Company's operations and ensuring legal compliance.

Objectives

1. To stipulate the principles and regulations 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 cyberattacks in any forms which may cause damages to the business operation of the Company.

Policy Composition

1. **Accountability, Identification and Authentication**

   1.1 Authentication is the process of verifying user’s identity for accessing the system.

   1.2 Authorization is specifying user’s rights/privileges to which menus they can use / or what they can do with the system.

   1.3 Accountability is recording the details of the application’s use, which the authentication procedures to access by the Company are specified as below;

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 / Token can access to the system, but 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.

2.8 And users must maintain the intact condition of the computer and equipment.

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

2.10 The user is responsible for preventing loss.

2.11 Do not install copyright infringement software and irrelevant software.

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 to access 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 covers the following stages:
   - Create an information system request form for the user to fill in the form for the access.
   - 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 appropriate.

3) Regarding 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 username 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 bringing Computers out of the working area. For example, the data in a computer sent for repair should be backed up and the data stored in the media must be deleted first.

4. Backup Policy

4.1 Make copies of data and software based on the priority of Information technology's data backup system.

4.2 Procedures for accurate data preparation, data backup and data restore must be utilized with software and technology systems, and the procedures are used differently based on the type of technology systems.

4.3 Backed-up information are kept in in the storage that must be specified with the name that can clearly present its software system, backup time and date, and the responsible person. The backup data should be stored in a backup storage installed at another location and require testing of storage media consistently.

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 and user groups such as Internal Zone and External Zone in order to systematically control and the cyberattacks preventing.

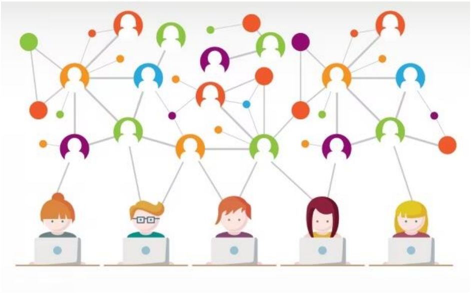
5.2 Users are prohibited to connect other computers and devices to the company's computers and network system unless users strictly obtain permission from the system administrator.

5.3 Prohibited actions include moving, installing, adding, or any modifications 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 to restrict user access rights to control service users to only access authorized network systems. There must be restriction method on access way to the shared Network.

5.5 All network systems of the organization that connect to other external networks should be connected through intrusion prevention devices, and they must have the capability to detect malicious software (Malware).

5.6 Internal IP address of the internal network system of the department require 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, 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 consist of at least 8 characters and contain lowercase and uppercase letters, a number and a symbol for more security.

2) Birth date, personal name, and self-related names should be avoided.

3) Dictionary words should not be used in your password whether it is a single word like home, or a compound word like Good Home, as hackers can use password cracking by comparing them from dictionary attack.

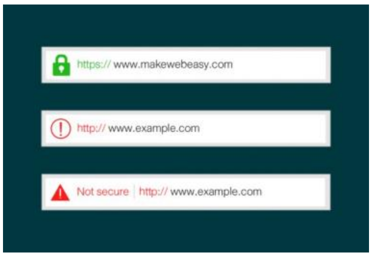
4) Different passwords are used for different accounts, especially for the access to important information --- the same password group can be used after differentiating the last number.

5) Some letters cannot be replaced with similar-looking numbers. For instances, the password is set as “H0use” by replacing the letter “O” with the number 0 (zero). It is still easy to guess even if 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.



https:// www.makewebeasy.com

http:// www.example.com

Not secure | http:// www.example.com

1) Always change your password (and username) when you turn on your devices. Remember to 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 leak to external source.
7) Install a Wi-Fi Router in the middle of the house because it provides more comprehensive signals and prevents hackers from breaking into signals to attack from outside.
8) Turn on the Firewall feature and install antivirus software to protect your devices on a Wi-Fi system.
9) Set up static IP for devices in your home to tighten scope of use and security.
10) Turn off the Wi-Fi Router when it is not being used, helps to reduce the risk of being attack and maintaining devices life.

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 medias.
4) Beware of the threats by opening files from various storage medias such as CD disk, flash drive, etc.
5) Always run a virus scan on your storage medias before use.
6) Do not open files with strange, unknown or suspicious extensions, such as .pif.
7) Do not use storage medias 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 segregate workplace section.

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

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

8.2.1 Fire Protection System

- Fire extinguisher containing an 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. Data Privacy

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.

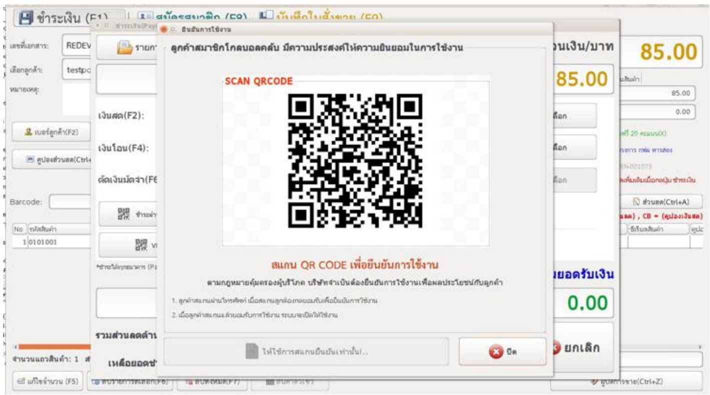
9.6 There are measures to keep personal data secure, such as encrypting important data.

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 storefront customers

การขอความยินยอมจากลูกค้าช่องทางหน้าร้าน



ยืนยันการใช้งาน

ลูกค้าสมาชิกโกลบอลคลับ มีความประสงค์ให้ความยินยอมในการใช้งาน

SCAN QRCODE

สแกน QR CODE เพื่อยืนยันการใช้งาน

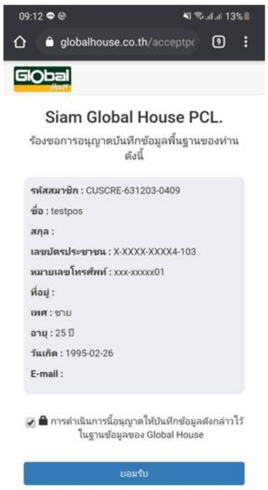
ตามกฎหมายคุ้มครองผู้บริโภค บริษัทจำเป็นต้องยืนยันการใช้งานเพื่อผลประโยชน์กับลูกค้า

1. ลูกค้าสแกนผ่านโทรศัพท์ เมื่อสแกนลูกค้าต้องกดยอมรับเพื่อยืนยันการใช้งาน

2. เมื่อลูกค้าสแกนและกดยอมรับการใช้งาน ระบบจะเปิดให้ใช้งาน

ให้ใช้การสแกนยืนยันเท่านั้น!...

ปิด



Siam Global House PCL.

ร้องขอการอนุญาตบันทึกข้อมูลพื้นฐานของท่านดังนี้

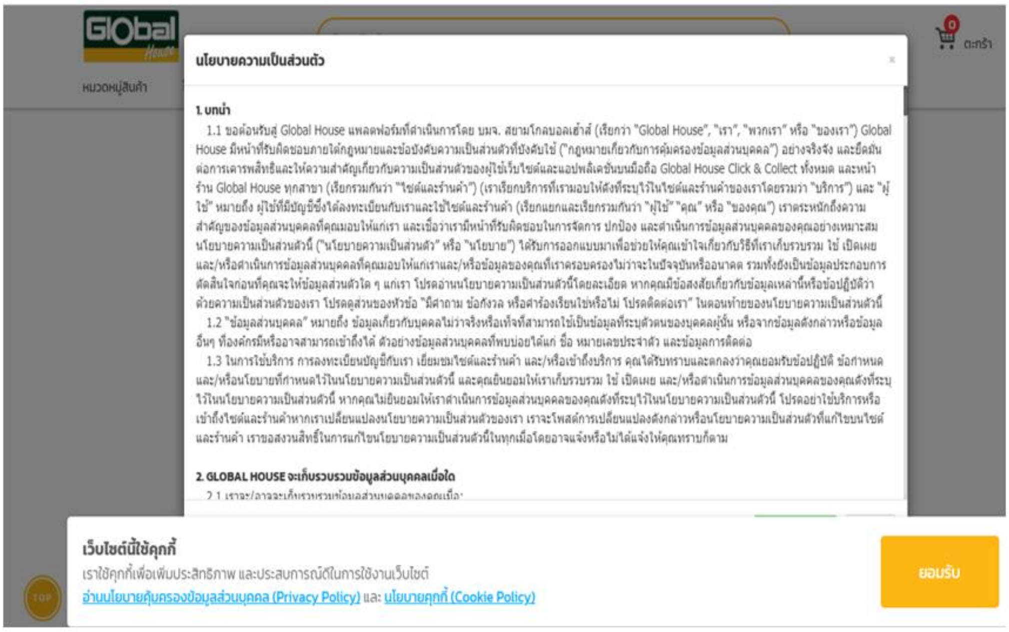
รหัสสมาชิก : CUSCRE-631203-0409
ชื่อ : testpos
สกุล :
เลขบัตรประชาชน : X-XXXX-XXXX4-103
หมายเลขโทรศัพท์ : xxx-xxxxx01
ที่อยู่ :
เพศ : ชาย
อายุ : 25 ปี
วันเกิด : 1995-02-26
E-mail :

☑ การดำเนินการนี้อนุญาตให้บันทึกข้อมูลดังกล่าวไว้ในฐานข้อมูลของ Global House

ยอมรับ

Requesting Consent from online customer

การขอความยินยอมจากลูกค้าช่องทางออนไลน์



นโยบายความเป็นส่วนตัว

1. บทนำ

1.1 ขอต้อนรับสู่ Global House แพลตฟอร์มที่ดำเนินการโดย บมจ. สยามโกลบอลเฮ้าส์ (เรียกว่า "Global House", "เรา", "พวกเรา" หรือ "ของเรา") Global House มีหน้าที่รับผิดชอบภายใต้กฎหมายและข้อบังคับความเป็นส่วนตัวที่บังคับใช้ ("กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล") อย่างจริงจัง และยึดมั่นต่อการเคารพสิทธิและให้ความสำคัญเกี่ยวกับความเป็นส่วนตัวของผู้ใช้เว็บไซต์และแอปพลิเคชันบนมือถือ Global House Click & Collect ทั้งหมด และหน้าร้าน Global House ทุกสาขา (เรียกรวมกันว่า "ไซต์และร้านค้า") (เราเรียกบริการที่เรามอบให้ดังที่ระบุไว้ในไซต์และร้านค้าของเราโดยรวมว่า "บริการ") และ "ผู้ใช้" หมายถึง ผู้ใช้ที่มีบัญชีซึ่งได้ลงทะเบียนกับเราและใช้ไซต์และร้านค้า (เรียกแยกและเรียกรวมกันว่า "ผู้ใช้" "คุณ" หรือ "ของคุณ") เราตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลที่คุณมอบให้แก่เรา และเชื่อว่าเรามีหน้าที่รับผิดชอบในการจัดการ ปกป้อง และดำเนินการข้อมูลส่วนบุคคลของคุณอย่างเหมาะสม นโยบายความเป็นส่วนตัวนี้ ("นโยบายความเป็นส่วนตัว" หรือ "นโยบาย") ได้รับการออกแบบมาเพื่อช่วยให้คุณเข้าใจเกี่ยวกับวิธีที่เราเก็บรวบรวม ใช้ เปิดเผย และ/หรือดำเนินการข้อมูลส่วนบุคคลที่คุณมอบให้แก่เราและ/หรือข้อมูลของคุณที่เราครอบครองไม่ว่าจะในปัจจุบันหรืออนาคต รวมทั้งยังเป็นข้อมูลประกอบการตัดสินใจก่อนที่คุณจะให้ข้อมูลส่วนตัวใด ๆ แก่เรา โปรดอ่านนโยบายความเป็นส่วนตัวนี้โดยละเอียด หากคุณมีข้อสงสัยเกี่ยวกับข้อมูลเหล่านี้หรือข้อปฏิบัติว่าด้วยความเป็นส่วนตัวของเรา โปรดดูส่วนของหัวข้อ "มีคำถาม ข้อกังวล หรือคำร้องเรียนใช่หรือไม่ โปรดติดต่อเรา" ในตอนท้ายของนโยบายความเป็นส่วนตัวนี้

1.2 "ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลไม่ว่าจริงหรือเท็จที่สามารถใช้เป็นข้อมูลที่ระบุตัวตนของบุคคลผู้นั้น หรือจากข้อมูลดังกล่าวหรือข้อมูลอื่นๆ ที่องค์กรมีหรืออาจสามารถเข้าถึงได้ ตัวอย่างข้อมูลส่วนบุคคลที่พบบ่อยได้แก่ ชื่อ หมายเลขประจำตัว และข้อมูลการติดต่อ

1.3 ในการใช้บริการ การลงทะเบียนบัญชีกับเรา เยี่ยมชมไซต์และร้านค้า และ/หรือเข้าถึงบริการ คุณได้รับทราบและตกลงว่าคุณยอมรับข้อปฏิบัติ ข้อกำหนด และ/หรือนโยบายที่กำหนดไว้ในนโยบายความเป็นส่วนตัวนี้ และคุณยินยอมให้เราเก็บรวบรวม ใช้ เปิดเผย และ/หรือดำเนินการข้อมูลส่วนบุคคลของคุณดังที่ระบุไว้ในนโยบายความเป็นส่วนตัวนี้ หากคุณไม่ยินยอมให้เราดำเนินการข้อมูลส่วนบุคคลของคุณดังที่ระบุไว้ในนโยบายความเป็นส่วนตัวนี้ โปรดอย่าใช้บริการหรือเข้าถึงไซต์และร้านค้าหากเราเปลี่ยนแปลงนโยบายความเป็นส่วนตัวของเรา เราจะโพสต์การเปลี่ยนแปลงดังกล่าวหรือนโยบายความเป็นส่วนตัวที่แก้ไขบนไซต์และร้านค้า เราขอสงวนสิทธิ์ในการแก้ไขนโยบายความเป็นส่วนตัวนี้ในทุกเมื่อโดยอาจแจ้งหรือไม่ได้แจ้งให้คุณทราบก็ตาม

2. GLOBAL HOUSE จะเก็บรวบรวมข้อมูลส่วนบุคคลเมื่อใด

2.1 เราจะ/อาจจะเก็บรวบรวมข้อมูลส่วนบุคคลของคุณเมื่อ:

เว็บไซต์นี้ใช้คุกกี้

เราใช้คุกกี้เพื่อเพิ่มประสิทธิภาพ และประสบการณ์ดีในการใช้งานเว็บไซต์

อ่านนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) และ นโยบายคุกกี้ (Cookie Policy)

ยอมรับ

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)

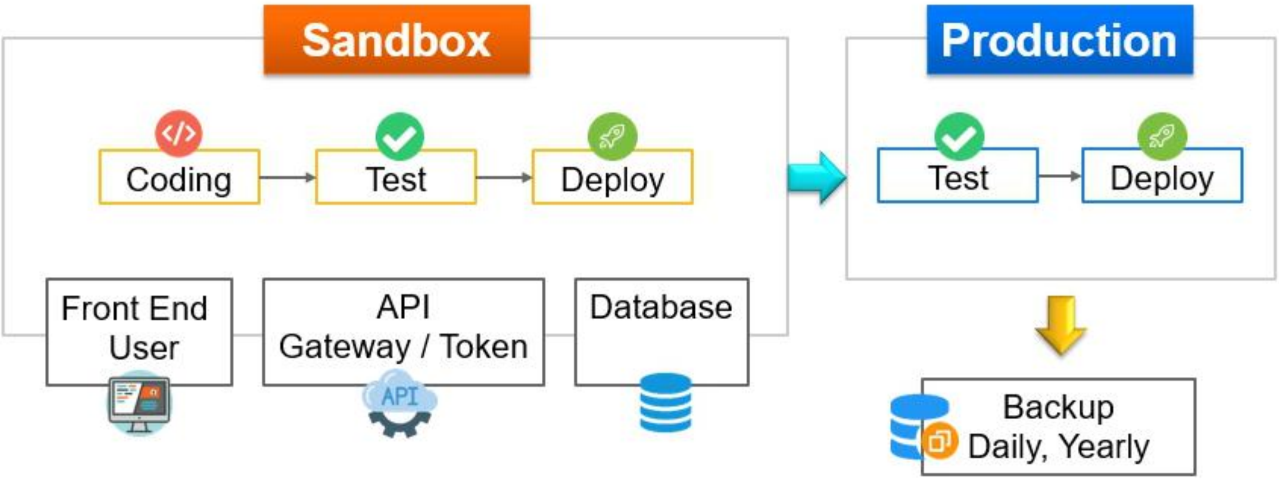
10.6 System Development and Testing Regulations

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

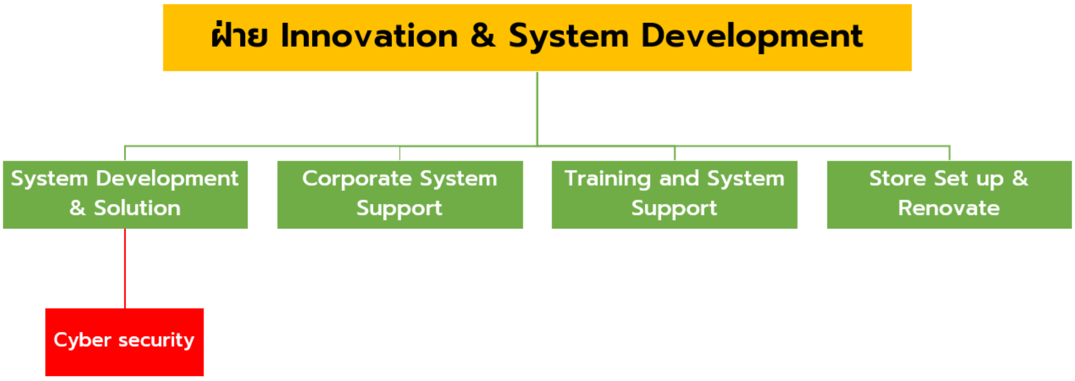
- Server API Gateway
- Database Server

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

Flow System Development



Innovation & System Development Department’s Chart


ฝ่าย Innovation & System Development
System Development & Solution
Corporate System Support
Training and System Support
Store Set up & Renovate
Cyber security

11. Cloud Usage and Cloud Security

11.1 Using authentication and security auditing

- Use the authentication system (Authentication), Users access the cloud only to authorized users.
- Regularly monitor security, checking activities within the cloud system, detecting any abnormalities that may occur.

11.2 Rights Management and Data Access

- Define access rights for each user level within the cloud.
- Encrypt data to protect stored information in the cloud and utilize encryption for communication between the cloud and users.

11.3 Risk Management and Monitoring

- Regularly assess and manage risks associated with the cloud.
- Implement intrusion detection systems to detect attacks and abnormalities in the cloud.

11.4 Compliance with Security Principles

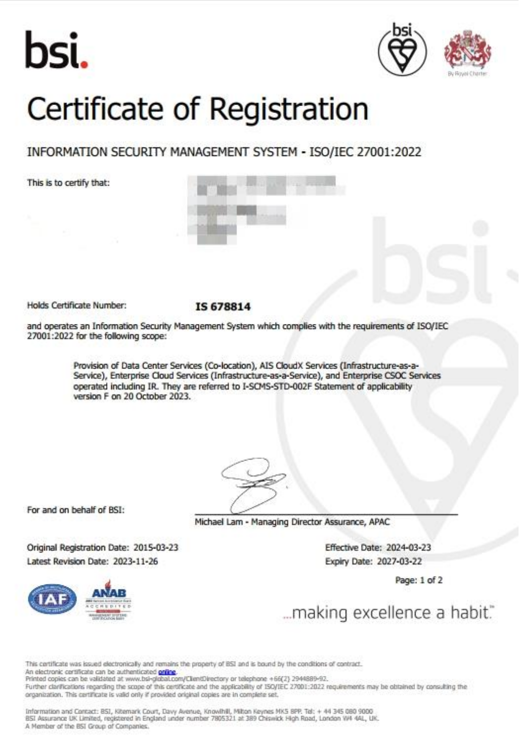
- Regularly update and maintain the security of the cloud system.
- Improvements and Upgrades operating systems and software used in the cloud.
- Establish data backup plans to ensure critical data stored in the cloud is not lost.

11.5 Training and Accountability

- Provide training for users on cloud security maintenance.
- Clearly define roles and responsibilities of personnel involved with the cloud.

Currently, the company uses cloud services that have the following security standards.

1. INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013



bsi.

By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2022

This is to certify that: [redacted]

Holds Certificate Number: **IS 678814**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope:

Provision of Data Center Services (Co-location), AIS CloudX Services (Infrastructure-as-a-Service), Enterprise Cloud Services (Infrastructure-as-a-Service), and Enterprise CSOC Services operated including IR. They are referred to I-SCMS-STD-002F Statement of applicability version F on 20 October 2023.

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2015-03-23
Latest Revision Date: 2023-11-26

Effective Date: 2024-03-23
Expiry Date: 2027-03-22

Page: 1 of 2

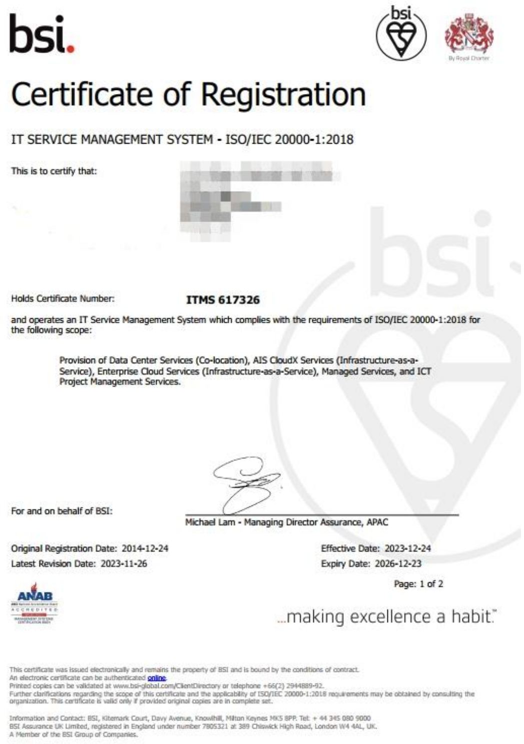
IAF ANAB ACCREDITED

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27001:2022 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

2. IT SERVICE MANAGEMENT SYSTEM - ISO/IEC 20000-1:2018



bsi.

By Royal Charter

Certificate of Registration

IT SERVICE MANAGEMENT SYSTEM - ISO/IEC 20000-1:2018

This is to certify that: [redacted]

Holds Certificate Number: **ITMS 617326**

and operates an IT Service Management System which complies with the requirements of ISO/IEC 20000-1:2018 for the following scope:

Provision of Data Center Services (Co-location), AIS CloudX Services (Infrastructure-as-a-Service), Enterprise Cloud Services (Infrastructure-as-a-Service), Managed Services, and ICT Project Management Services.

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2014-12-24
Latest Revision Date: 2023-11-26

Effective Date: 2023-12-24
Expiry Date: 2026-12-23

Page: 1 of 2

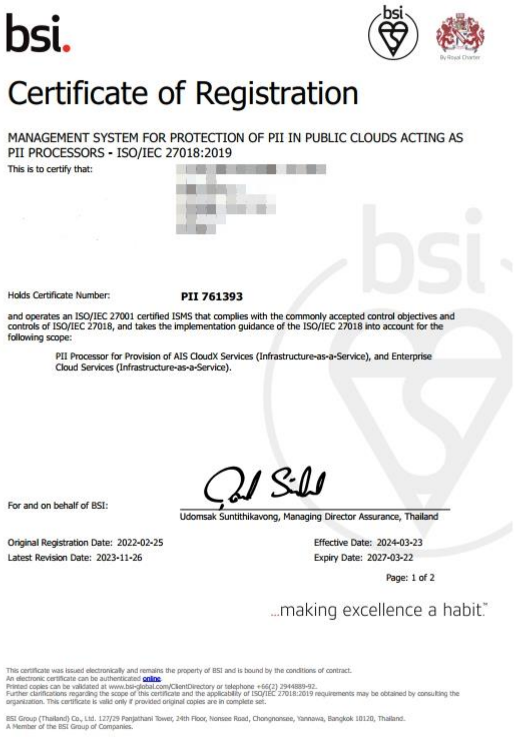
ANAB ACCREDITED

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 20000-1:2018 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

3. MANAGEMENT SYSTEM FOR PROTECTION OF PII IN PUBLIC CLOUDS ACTING ASPII PROCESSORS - ISO/IEC 27018:2019



bsi.

By Royal Charter

Certificate of Registration

MANAGEMENT SYSTEM FOR PROTECTION OF PII IN PUBLIC CLOUDS ACTING AS PII PROCESSORS - ISO/IEC 27018:2019

This is to certify that: [redacted]

Holds Certificate Number: **PII 761393**

and operates an ISO/IEC 27001 certified ISMS that complies with the commonly accepted control objectives and controls of ISO/IEC 27018, and takes the implementation guidance of the ISO/IEC 27018 into account for the following scope:

PII Processor for Provision of AIS CloudX Services (Infrastructure-as-a-Service), and Enterprise Cloud Services (Infrastructure-as-a-Service).

For and on behalf of BSI:

Udomsak Suntithikavong, Managing Director Assurance, Thailand

Original Registration Date: 2022-02-25
Latest Revision Date: 2023-11-26

Effective Date: 2024-03-23
Expiry Date: 2027-03-22

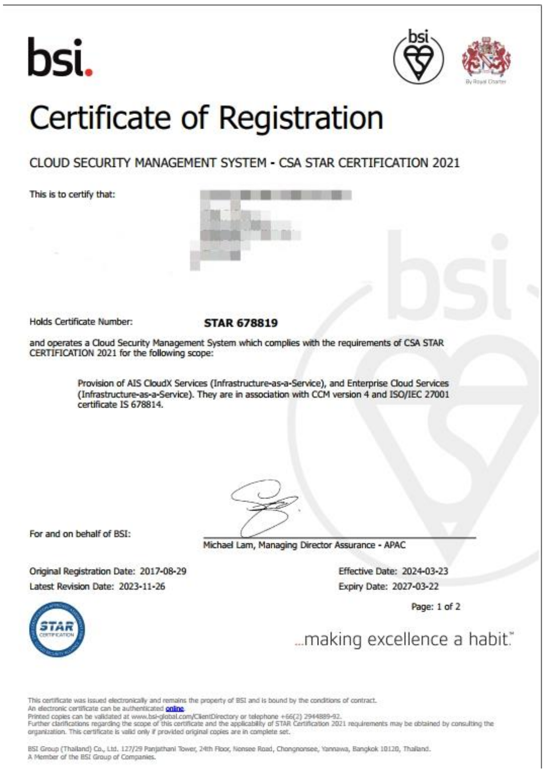
Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27018:2019 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

BSI Group (Thailand) Co., Ltd. 127/29 Panjathani Tower, 24th Floor, Nonsee Road, Chongnonsee, Yannawa, Bangkok 10120, Thailand.
A Member of the BSI Group of Companies.

4. CLOUD SECURITY MANAGEMENT SYSTEM - CSA STAR CERTIFICATION 2021



bsi.

By Royal Charter

Certificate of Registration

CLOUD SECURITY MANAGEMENT SYSTEM - CSA STAR CERTIFICATION 2021

This is to certify that: [redacted]

Holds Certificate Number: **STAR 678819**

and operates a Cloud Security Management System which complies with the requirements of CSA STAR CERTIFICATION 2021 for the following scope:

Provision of AIS CloudX Services (Infrastructure-as-a-Service), and Enterprise Cloud Services (Infrastructure-as-a-Service). They are in association with CCM version 4 and ISO/IEC 27001 certificate IS 678814.

For and on behalf of BSI:

Michael Lam, Managing Director Assurance - APAC

Original Registration Date: 2017-08-29
Latest Revision Date: 2023-11-26

Effective Date: 2024-03-23
Expiry Date: 2027-03-22

Page: 1 of 2

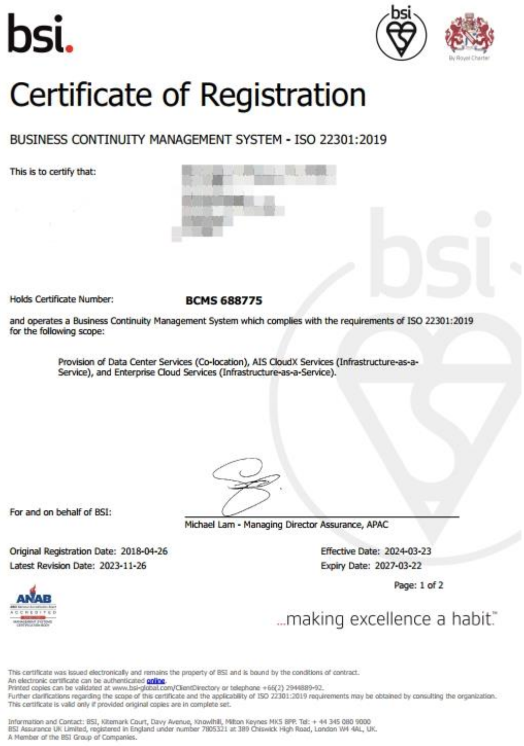
STAR CERTIFICATION

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of STAR Certification 2021 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

BSI Group (Thailand) Co., Ltd. 127/29 Panjathani Tower, 24th Floor, Nonsee Road, Chongnonsee, Yannawa, Bangkok 10120, Thailand.
A Member of the BSI Group of Companies.

5. BUSINESS CONTINUITY MANAGEMENT SYSTEM - ISO 22301:2019



bsi.

Certificate of Registration

BUSINESS CONTINUITY MANAGEMENT SYSTEM - ISO 22301:2019

This is to certify that: [redacted]

Holds Certificate Number: **BCMS 688775**

and operates a Business Continuity Management System which complies with the requirements of ISO 22301:2019 for the following scope:

Provision of Data Center Services (Co-location), AIS CloudX Services (Infrastructure-as-a-Service), and Enterprise Cloud Services (Infrastructure-as-a-Service).

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2018-04-26
Latest Revision Date: 2023-11-26

Effective Date: 2024-03-23
Expiry Date: 2027-03-22

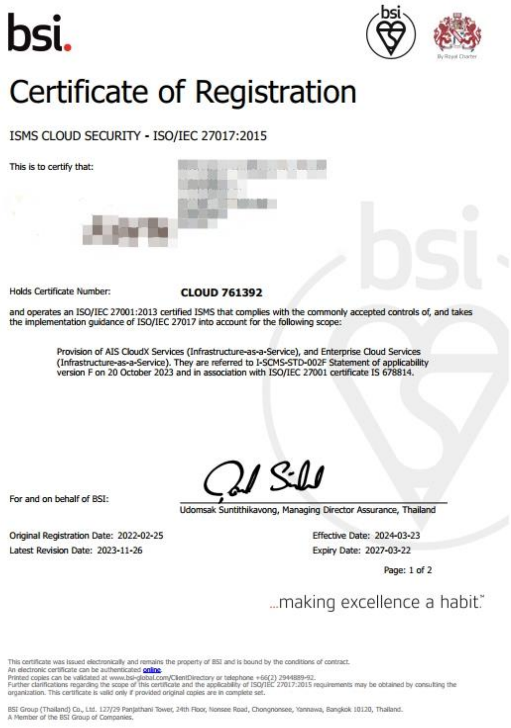
Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of ISO 22301:2019 requirements may be obtained by consulting the organization.
This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

6. ISMS CLOUD SECURITY - ISO /IEC 27017:2015



bsi.

Certificate of Registration

ISMS CLOUD SECURITY - ISO/IEC 27017:2015

This is to certify that: [redacted]

Holds Certificate Number: **CLOUD 761392**

and operates an ISO/IEC 27001:2013 certified ISMS that complies with the commonly accepted controls of, and takes the implementation guidance of ISO/IEC 27017 into account for the following scope:

Provision of AIS CloudX Services (Infrastructure-as-a-Service), and Enterprise Cloud Services (Infrastructure-as-a-Service). They are referred to I-SCMS-STD-002F Statement of applicability version F on 20 October 2023 and in association with ISO/IEC 27001 certificate IS 678814.

For and on behalf of BSI:

Udomsak Suntithikavong, Managing Director Assurance, Thailand

Original Registration Date: 2022-02-25
Latest Revision Date: 2023-11-26

Effective Date: 2024-03-23
Expiry Date: 2027-03-22

Page: 1 of 2

...making excellence a habit.™

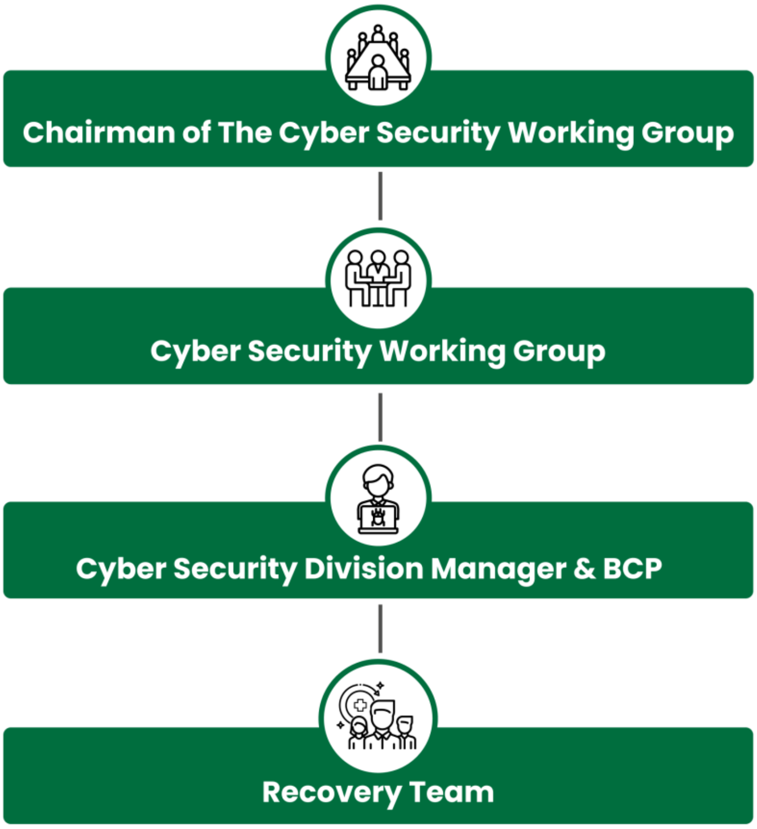
This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27017:2015 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

BSI Group (Thailand) Co., Ltd. 127/29 Panjathani Tower, 24th Floor, Nonsee Road, Chongnonsee, Yannawa, Bangkok 10120, Thailand.
A Member of the BSI Group of Companies.

12. Business Continuity and Disaster Recovery

Business Continuity

The company aims to maintain services and operations during and after events that cause interruptions, such as natural disasters, cyber-attacks, power outages, or equipment failures. The goals of the company's business continuity planning include reducing downtime, protecting critical data and systems, and ensuring that the company and its key resources are quickly restored and able to resume normal operations.



Chairman of The Cyber Security Working Group

Cyber Security Working Group

Cyber Security Division Manager & BCP

Recovery Team

IT Business Continuity Planning

1. **Risk Assessment:** The company assesses risks and threats that could lead to disruptions in IT services, such as hardware or software failures, security breaches, or natural disasters. The Company will evaluate the potential impact of these events on its operations.
2. **Business Impact Analysis:** The company identifies critical IT systems and necessary applications for business operations. It evaluates the financial impact and operational implications of potential IT disruptions.
3. **Business Continuity Plan (BCP):** The company develops a comprehensive plan outlining steps to be followed during a disruption, backup and recovery strategies, infrastructure and alternative systems, communication plans, and roles and responsibilities of the IT team.

4. **Data Backup and Recovery:** The company implements regular data backup procedures. That critical data is protected and recoverable in case of disruptions. Test data recovery processes to verify their effectiveness.
5. **Incident Response:** The company establishes teams and procedures for detecting, responding to, and mitigating IT-related incidents, including cybersecurity threats, security breaches, and restoring systems to normal operation.

6. **Testing and Training:** The company mandates testing of the Business Continuity Plan (BCP) regarding information systems and cybersecurity at least once a year, including relevant scenarios, to ensure the IT team is familiar with their roles and responsibilities during disruptions.
7. **Service Provider Management:**The company assesses the business continuity plans of key service providers, and establishes clear Service Level Agreements (SLAs) to ensure readiness and service recovery.
8. **Communication and Stakeholder Management:** The company establishes communication channels and protocols to keep stakeholders informed during disruptions, including internal communication within the organization and external communication with customers, partners, and regulatory agencies.
9. **Communication and Stakeholder Management:** The company establishes communication channels and protocols to keep stakeholders informed during disruptions, including internal communication within the organization and external communication with customers, partners, and regulatory agencies.

Disaster Recovery

Business continuity planning emphasizes restoring IT systems, applications, and data, especially after disruptions. The company's business continuity planning addresses the broader aspect of maintaining operations during and after a disruption. Disaster recovery involves technical recovery and restoration of IT infrastructure specifically.

Key Components and Considerations of the Disaster Recovery Plan:

1. **Data Backup and Recovery Strategy:** The company defines suitable data backup strategies for its IT systems and data, which may include regular backups to off-site storage or the cloud storage, and replicate critical systems to both types of storage, and defines recovery point objectives (RPO) and recovery time objectives (RTO) to define

acceptable limits for data loss and downtime.

2 . Data Replication and Redundancy: The company utilizes technologies such as data replication and mirroring to maintain real-time copies of data. This ensures that if one system or location fails, there will be a backup copy available for recovery.

3. Disaster Recovery Site: The company identifies and backs up storage or data centers that can replicate and activate critical IT systems and infrastructure in the case of a disaster. These sites have the necessary infrastructure, connectivity, and resources for operational recovery.

4. System Recovery Team: The company establishes dedicated teams responsible for managing and executing the system recovery plan. Assign roles and responsibilities to team members, ensuring they are trained and prepared to efficiently perform their duties.

5. Recovery Procedure: The company develops detailed procedures for IT system, application, and data recovery. These procedures include step-by-step guidance for system initiation, data restoration, and testing.

6 . Testing and Maintenance: : The company tests its disaster recovery plans regularly to check their effectiveness, performing both partial and full-scale simulations to simulate various disaster scenarios. It checks hardware, software, and backup systems and ensures they are regularly maintained and updated.

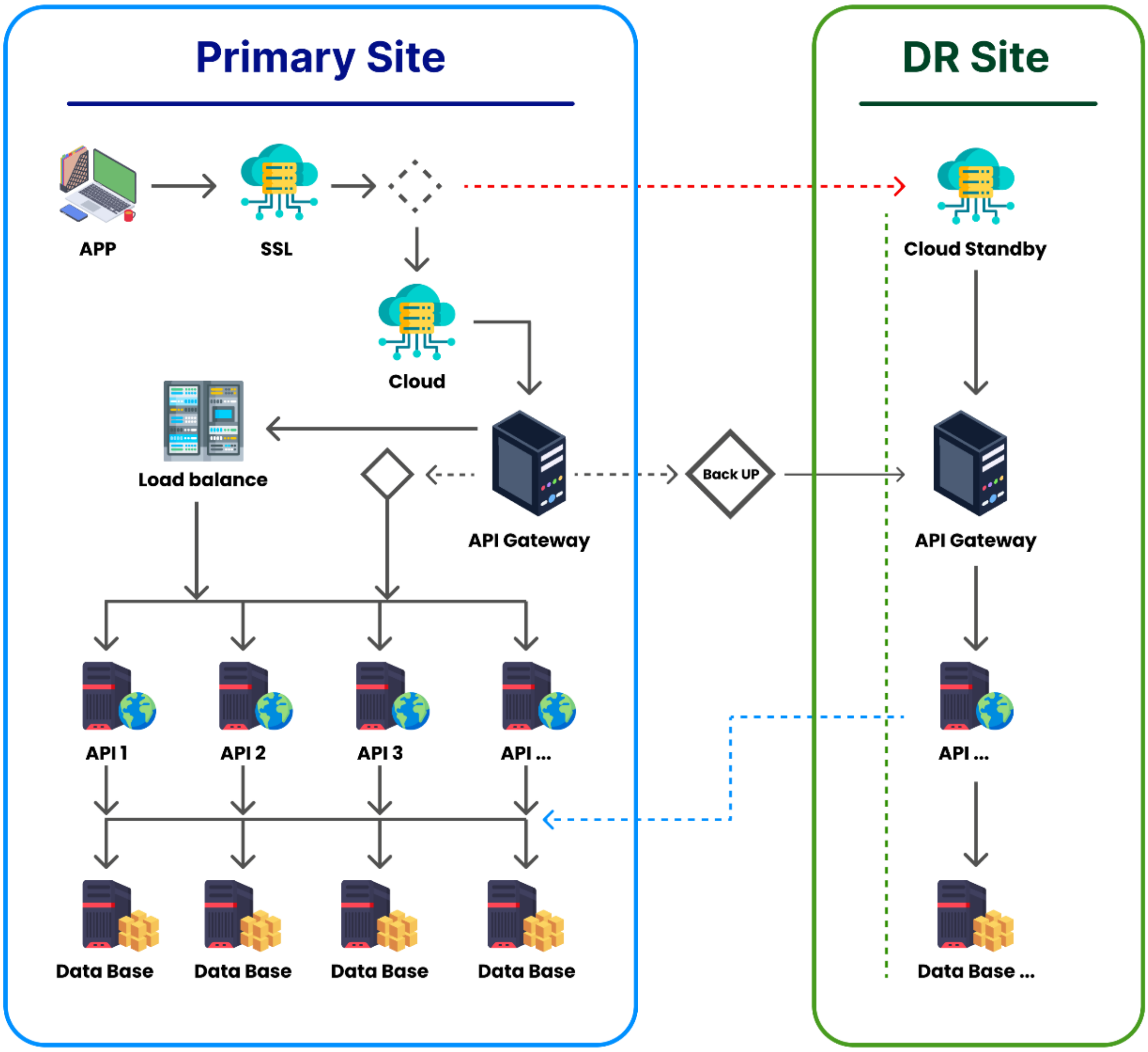
7. Communication and Coordination: The company establishes clear communication channels and protocols for efficient coordination among team members during disasters and determines methods for disseminating the latest information to stakeholders, including employees, customers, and partners.

8 . Documentation and Version Control: The company prepares accurate up-to-date documentation of the disaster recovery plan, including network diagrams and contact information, ensuring easy access for involved team members.

9 . Collaboration with Vendors and Suppliers: The company collaborates with vendors and third-party service providers to ensure readiness during recovery and create agreements and Service Level Agreements (SLAs) that define roles and responsibilities clearly in case of a disaster.

10. Continuous Improvement: The company regularly reviews and updates its disaster recovery plan based on lessons learned from various scenario tests every six months and makes changes to the IT infrastructure to stay updated with emerging technologies and best practices to improve the efficiency of the recovery plan.

Disaster Recovery (*DR Site*) for Business Continuity

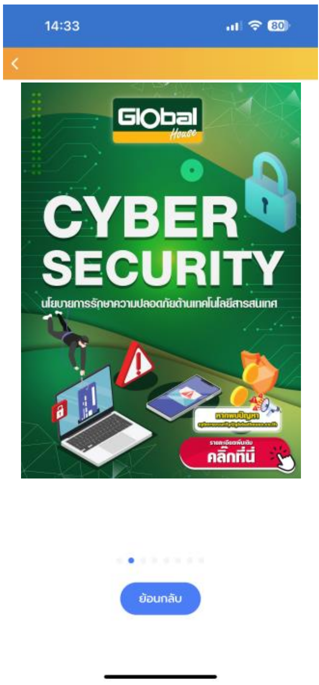


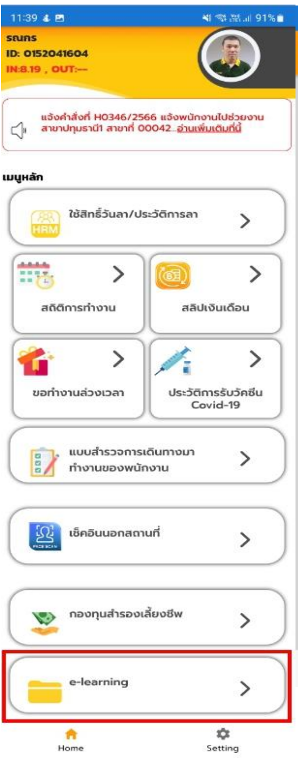
13. Cyber Security Measure and Cyberattack Response

Apart from the aforementioned measures, the employees can inquire about abnormalities and report damages from attacking Cyber Security through the IT Service Center - reporting to the email cybersecurity@globalhouse.co.th Then, complying with the Incident Report and Escalation Process, Technology officers will take care of such reports. In this regard, communication and reporting will be given to those involved to take action -- from the operating position level to the senior executives -- including following up until the issues are resolved.

Cyber Security Communication and Education

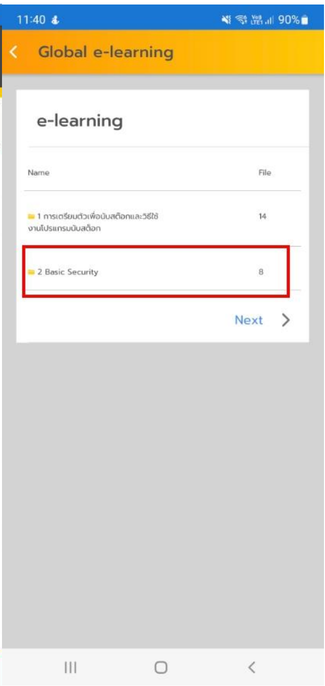
The company informs, communicates, and educates all employees about cyber security and the employees' and company's privacy, enabling them to acknowledge cyber dangers, through the Agilis HR application. All of them can access E-learning and, at least once a year, they must be trained in cyber security.


14:33


11:39 91%

ธนกร
ID: 0152041604
IN:8.19 , OUT:--

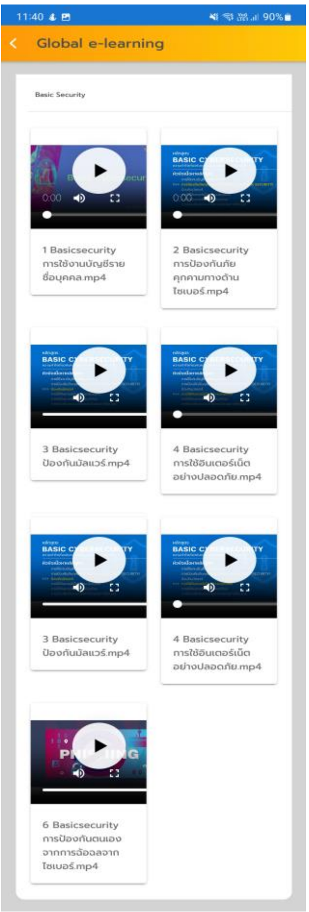
แจ้งคำสั่งที่ H0346/2566 แจ้งพนักงานไปช่วยงาน สาขาปทุมธานี1 สาขาที่ 00042...อ่านเพิ่มเติมที่นี่


11:40 90%

Global e-learning

e-learning

Name	File
1 การเตรียมตัวเพื่อนับสต๊อกและวิธีใช้งานโปรแกรมนับสต๊อก	14
2 Basic Security	8


11:40 90%

Global e-learning

Basic Security

1 Basicsecurity การใช้งานบัญชีรายชื่อบุคคล.mp4

2 Basicsecurity การป้องกันภัยคุกคามทางด้านไซเบอร์.mp4

3 Basicsecurity ป้องกันมัลแวร์.mp4

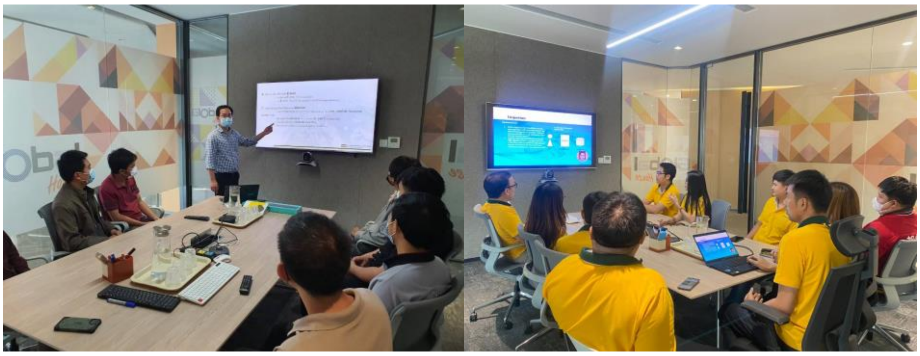
4 Basicsecurity การใช้อินเตอร์เน็ตอย่างปลอดภัย.mp4

3 Basicsecurity ป้องกันมัลแวร์.mp4

4 Basicsecurity การใช้อินเตอร์เน็ตอย่างปลอดภัย.mp4

6 Basicsecurity การป้องกันตนเองจากการฉ้อฉลจากไซเบอร์.mp4

To enhance knowledge, the company provides training and seminars on cybersecurity, the company's security policy, cyber risk assessment, and safety management within the organization.



Cyber Security Communication and Education is a continuing process, as technological changes and cyber dangers always happen. Nevertheless, awareness and prevention of cyber security is an important matter that the company pays attention to, and constantly develops knowledge and skills in this area.

14. **Cyber offenses within the organization**

14.1 Use the other user’s password or the other user's identity or the One Time Password: OTP to sign in to the company’s computer system with the purpose of reading, copying, approving, editing, changing, and deleting data, whether for personal gain or that of others, negligently. Use a password, user identification, or one-time password of the others, or intentionally let others use that password, or user ID and rights to use one's computer system.

14.2 Reveal concealed business information or knowledge of the Company to others without permission from the Company. Intentionally steal or use company information to disclose, sell, or distribute to others for personal gain, which causes damage to the company.

14.3 Steal or forge passwords or other users' identity data to deliberately log into the computer system to commit fraud against the company's or customers' assets or damage their reputation.

14.4 Copy or possess inappropriate or illegal materials, such as texts, pornographic images, or any other items that insult the nation, religion, and monarchy, incite division among the public or employees, or cause damage to the company.

14.5 Steal, hack, eavesdrop, route, or decode electronic data by using any other tools or technology to obtain information or secrets of other people or the company with the intent to cause damage to other people or the company.

14.6 Be careless, neglect, or overlook the situation that causes other people to steal or reveal the company's information, sell, distribute, and attempt to gain access to systems that they do not have permission to or are not allowed to use intentionally. Or intend to disturb/destroy information computer systems or various equipment to cause damage to the company.

14.7 Install or use hacking tools or other software involving verification and access to the important data of the company. But such action is except for persons or agencies specifically responsible for the security of information technology systems.

14.8 Connect computer devices or other electronic devices to the company's computer system or network without authorization from the responsible department; set and install or change the IP address by oneself without authorization from the responsible department; modify, alter, or move components of the computer system arbitrarily; or connect or install additional computer equipment that is not the company's property without authorization.

14.9 Send inappropriate messages or information through the company's email system or communication tools for defamation, harassment, extortion, slander, insults, or chain letters; use the Internet, Intranet, or E-mail for purposes unrelated to the company's business; and use the company's computers and other equipment for personal entertainment or benefit.

14.10 Use software without legal licensing or without the company's permission, or that may cause damage to the company.

14.11 Assist or cooperate with outsiders to access the company's computer or information system, or copy or destroy the company's information or computer systems.

15. Penalties for committing cyber offenses within an organization

15.1 Verbal warning

15.2 Written warning

15.3 Temporary suspension without pay

15.4 Discharge

15.5 Expulsion

15.6 Criminal or civil proceedings

The company are not required to follow the above sequence, and may choose the punishment differently, depending on the severity of the committed offense.

16. Development and Change/modification Policy of information systems

16.1. Introduction

The policy establishes guidelines and procedures for developing, changing, and modifying information systems within the organization, ensuring that any changes are effective, secure, and aligned with the organization's strategy and goals.

16.2. Scope

The policy covers all information systems used within the organization, whether developed internally or purchased from external sources.

16.3. Responsibilities

Requestor: Individuals seeking to develop, change, or modify information systems.

Review Committee: The person assigned to consider the request. It consists of representatives from IT, business, and other relevant departments.

Developer: The person responsible for developing, changing, and modifying the information system.

Administrator: A person responsible for maintaining and supporting the use of information systems.

16.4. Request Procedure

16.4.1 The requester must fill out an electronic form for the development, modification, or correction of the information system, which must include the following details:

-Subject/Topic

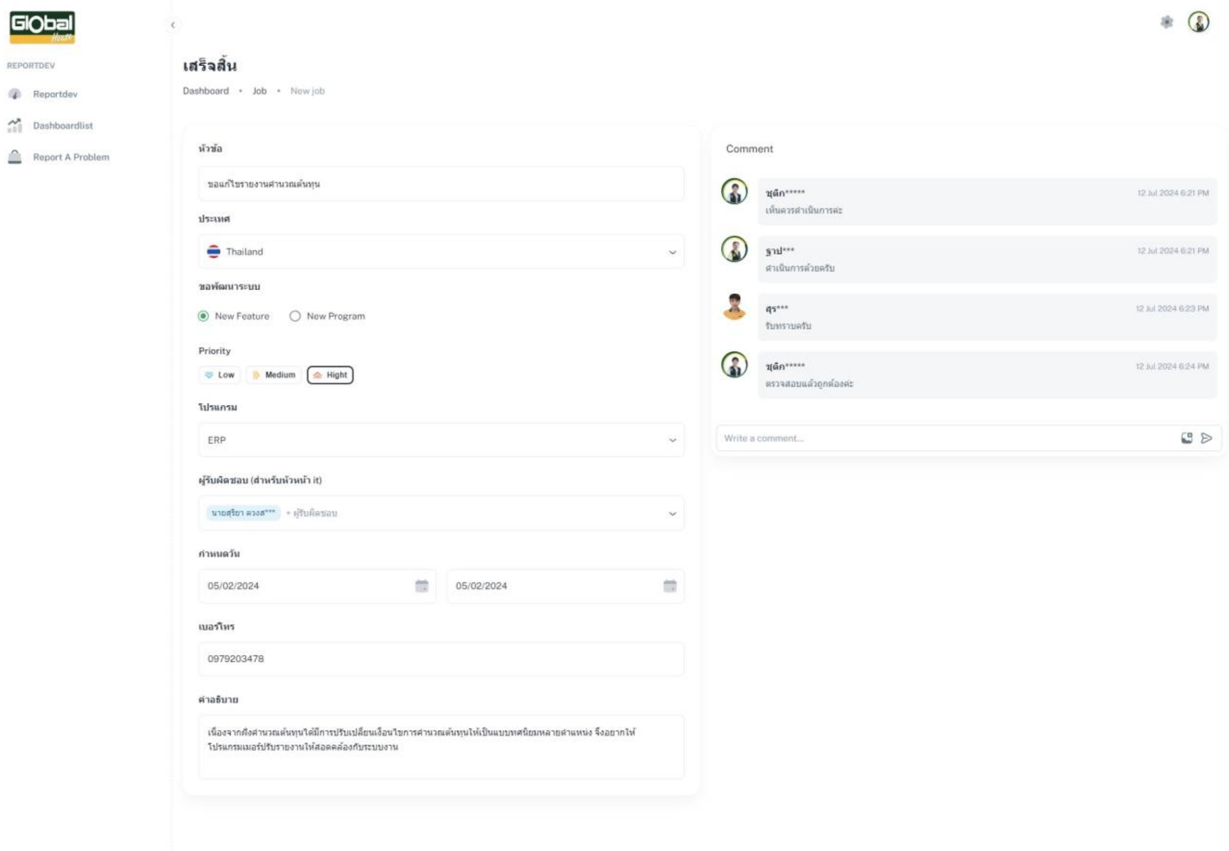
-Priority

-Purpose of the Change

-Expected Impacts

-Contact Person

Example



เสร็จสิ้น

Dashboard • Job • New job

หัวข้อ
ขอแก้ไขรายงานคำนวณต้นทุน

ประเทศ
Thailand

ขอพัฒนาระบบ
● New Feature ○ New Program

Priority
Low Medium [✓ Hight]

โปรแกรม
ERP

ผู้รับผิดชอบ (สำหรับหัวหน้า it)
นายสุริยา ดวงส*** + ผู้รับผิดชอบ

กำหนดวัน
05/02/2024 05/02/2024

เบอร์โทร
0979203478

คำอธิบาย
เนื่องจากฝั่งคำนวณต้นทุนได้มีการปรับเปลี่ยนเงื่อนไขการคำนวณต้นทุนให้เป็นแบบทศนิยมหลายตำแหน่ง จึงอยากให้โปรแกรมเมอร์ปรับรายงานให้สอดคล้องกับระบบงาน

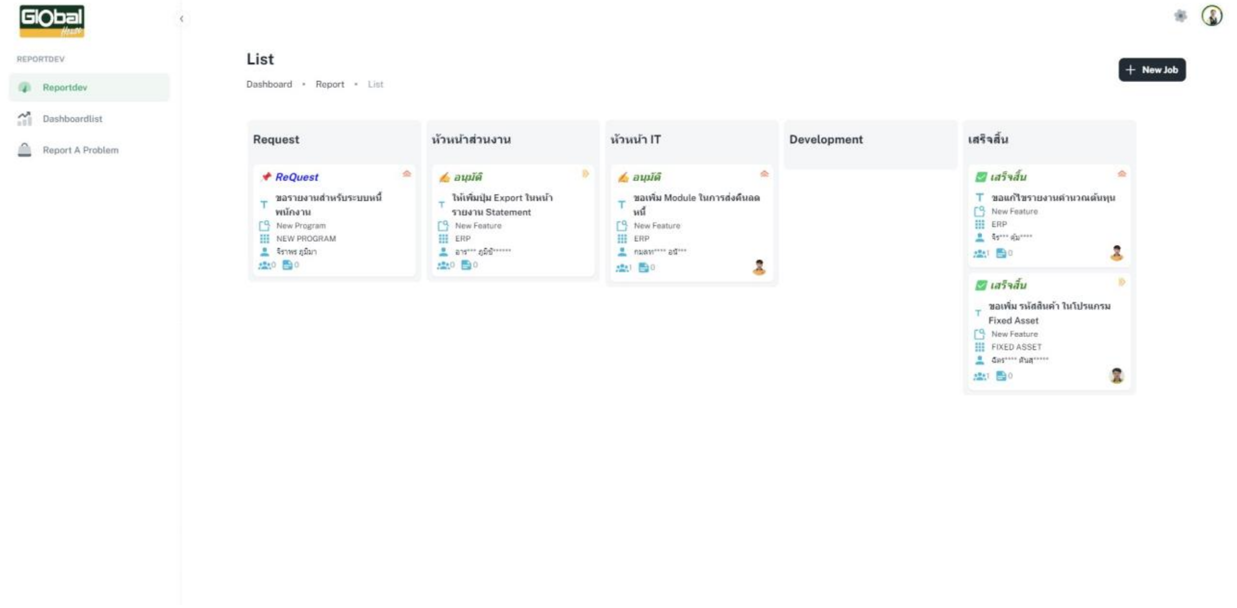
Comment

ชุติก***** 12 Jul 2024 6:21 PM
เห็นควรดำเนินการค่ะ

ฐาป*** 12 Jul 2024 6:21 PM
ดำเนินการด้วยครับ

สุร*** 12 Jul 2024 6:23 PM
รับทราบครับ

ชุติก***** 12 Jul 2024 6:24 PM
ตรวจสอบแล้วถูกต้องค่ะ



REPORTDEV

Reportdev

Dashboardlist

Report A Problem

List

Dashboard • Report • List

+ New Job

Request

ReQuest
ขอรายงานสำหรับระบบหนี้พนักงาน
New Program
NEW PROGRAM
จิราพร ภูมิมา
0 0

หัวหน้าส่วนงาน

อนุมัติ
ให้เพิ่มปุ่ม Export ในหน้ารายงาน Statement
New Feature
ERP
อาร*** ภูมิช******
0 0

หัวหน้า IT

อนุมัติ
ขอเพิ่ม Module ในการส่งคืนลดหนี้
New Feature
ERP
กมลท**** อนี***
1 0

Development

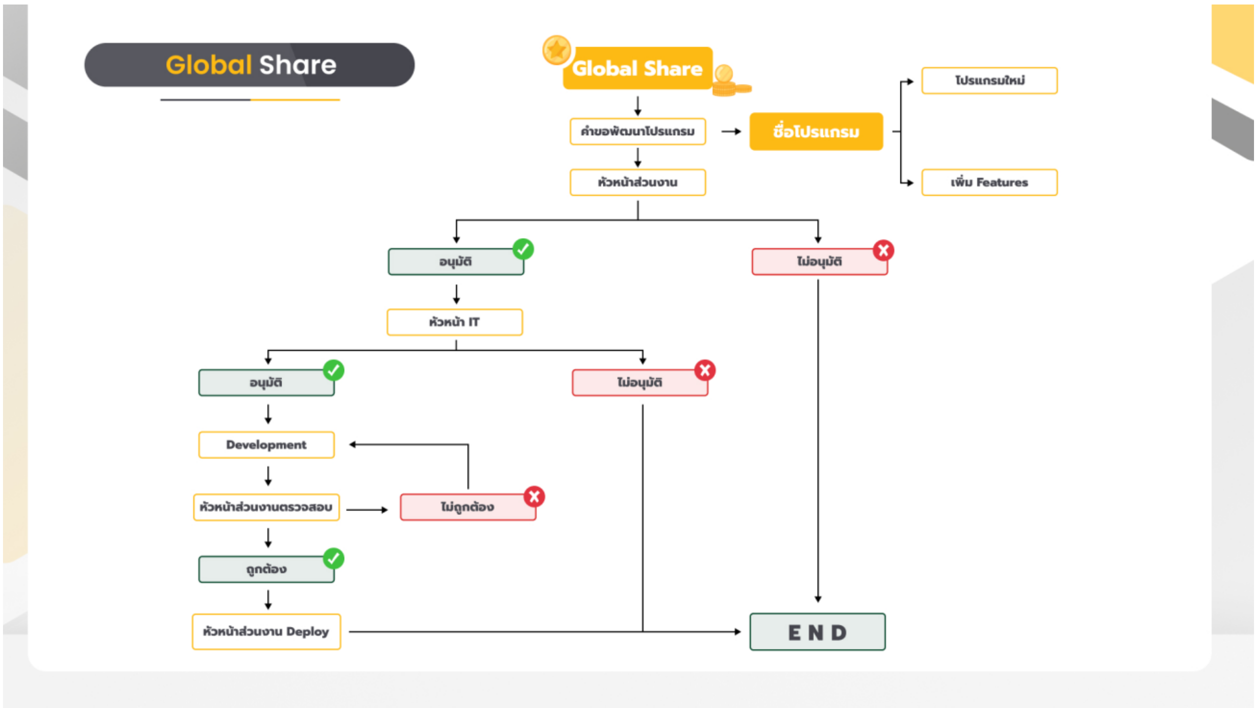
เสร็จสิ้น

เสร็จสิ้น
ขอแก้ไขรายงานคำนวณต้นทุน
New Feature
ERP
จิร*** คุ้ม****
1 0

เสร็จสิ้น
ขอเพิ่ม รหัสสินค้า ในโปรแกรม Fixed Asset
New Feature
FIXED ASSET
ฉัตร**** คันสุ*****
1 0

16.4.2 Scope

The policy covers all information systems used within the organization, whether developed internally or purchased from external sources.



16.4.3 The review committee will evaluate the request and decide whether to approve it.

Evaluation criteria:

- Alignment with organizational strategy and goals
- Necessity and urgency

- Impact on users
- Available resources
- Risks

16.4.4 If the Review Committee approves the request, the developer is responsible for implementing the approved development, change, or modification of the information system.

17. Management of incidents that may affect information use

17.1. Introduction

This policy stipulates the procedure of Incident Management within the organization to ensure that the incidents are identified, analyzed, responded to, and closed - minimizing the effects and securing the data.

17.2. Frame

This policy covers all events that may affect the organization's information systems, data, or operations, including:

- Cyber threats such as DDoS attacks, phishing attacks, and data leaks
- System failure, such as a server crash, application malfunction, and network failure
- Natural disasters such as floods, fires, and earthquakes
- Other accidents such as power outages and damaged equipment.

17.3 Responsible person

Incident Reporting Team: responsible for receiving incident reports, starting the event management process, and coordinating with other teams.

Incident Analysis Team: identifying the cause of the incident, assessing the impact, and collecting relevant information

Incident Response Team: resolving incidents, recovering systems, and preventing incidents from happening again.

Board: deciding on a course of action, allocating resources, and communicating with stakeholders.

17.4 Incident management procedure

17.4.1 Notification of events

Users or related persons can report incidents through many channels such as telephone, email, LINE, and Global share system. The incident team records primary information about the incident, assesses the severity, and sets the level of importance.

17.4.2 Event analysis

the incident analysis team will collect additional information about the incident for analysis, assess the impact, and specify how to fix it. The incident analysis team may need to interview users, check system logs, or test the system to find the cause.

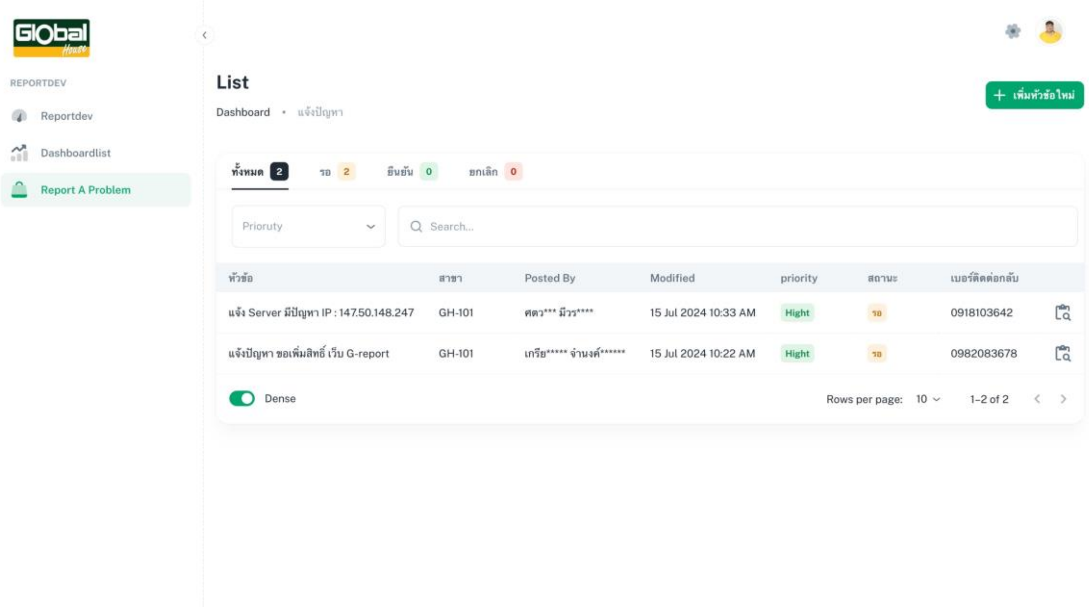
17.4.3 Incident Response

the Incident Response Team will resolve the incident according to the established plan. This may include system recovery, blocking attacks, or data migration. The incident response team communicates with users about the status of the incident and informs them when the incident is resolved.

17.4.4 Closing the event

when the incident is resolved, the event analysis team records lessons learned from the event, specifies guidelines to prevent the incident, and recommends improvements to the incident management process. The incident team will close the incident in the system.

Example of incident recording screen

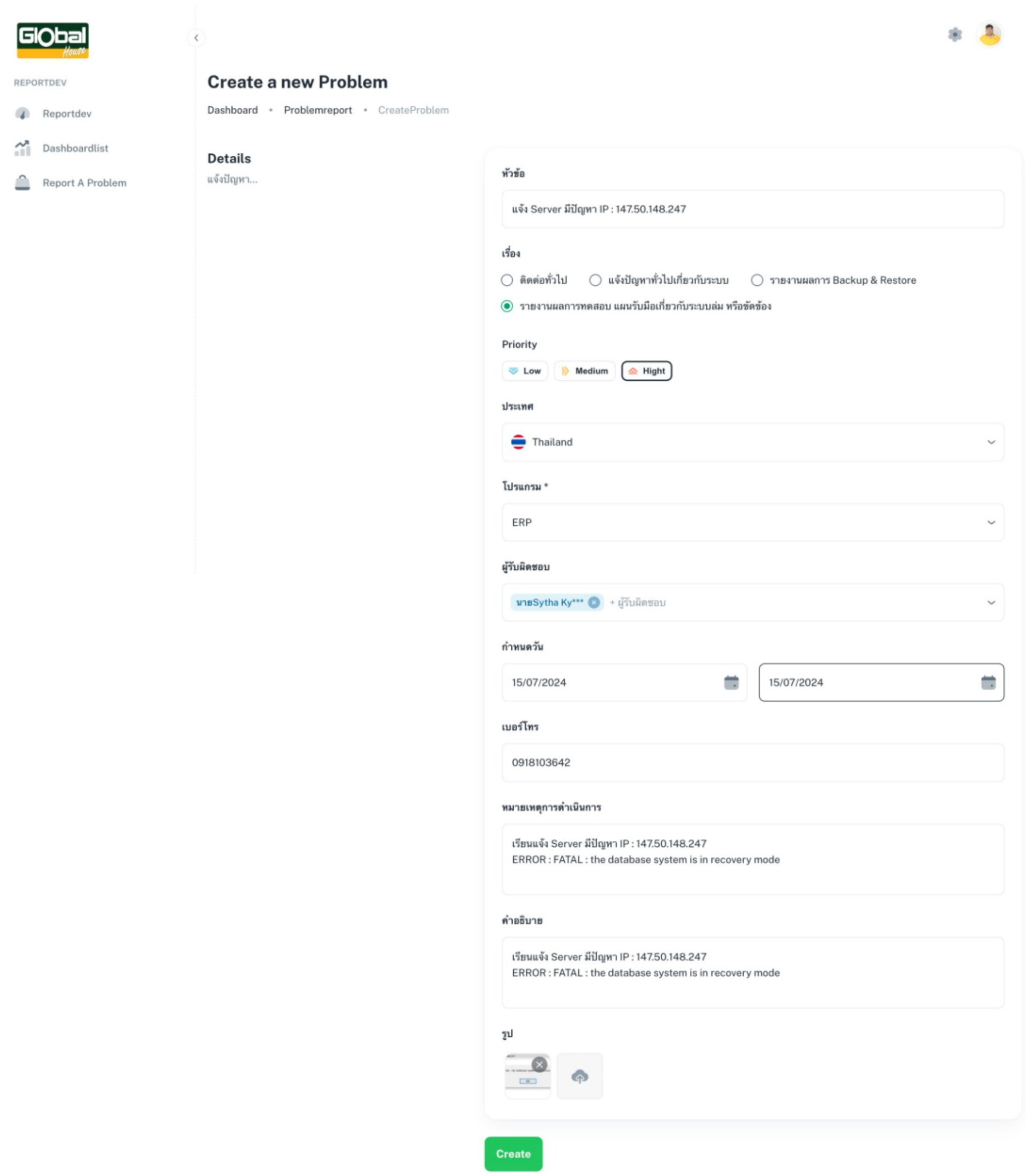


List

Dashboard • แจ้งปัญหา

หัวข้อ	สาขา	Posted By	Modified	priority	สถานะ	เบอร์ติดต่อกลับ
แจ้ง Server มีปัญหา IP : 147.50.148.247	GH-101	ศดว*** มีวร****	15 Jul 2024 10:33 AM	Hight	รอ	0918103642
แจ้งปัญหา ขอเพิ่มสิทธิ์ เว็บ G-report	GH-101	เกรีย***** จำนงค์******	15 Jul 2024 10:22 AM	Hight	รอ	0982083678

Rows per page: 10 1–2 of 2



Create a new Problem

Dashboard • Problemreport • CreateProblem

Details
แจ้งปัญหา...

หัวข้อ
แจ้ง Server มีปัญหา IP : 147.50.148.247

เรื่อง
○ ติดต่อทั่วไป ○ แจ้งปัญหาทั่วไปเกี่ยวกับระบบ ○ รายงานผลการ Backup & Restore
● รายงานผลการทดสอบ แผนรับมือเกี่ยวกับระบบล่ม หรือขัดข้อง

Priority
Low Medium [✓ Hight]

ประเทศ
Thailand

โปรแกรม *
ERP

ผู้รับผิดชอบ
นายSytha Ky*** + ผู้รับผิดชอบ

กำหนดวัน
15/07/2024 15/07/2024

เบอร์โทร
0918103642

หมายเหตุการดำเนินการ
เรียนแจ้ง Server มีปัญหา IP : 147.50.148.247
ERROR : FATAL : the database system is in recovery mode

คำอธิบาย
เรียนแจ้ง Server มีปัญหา IP : 147.50.148.247
ERROR : FATAL : the database system is in recovery mode

รูป

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

Company Limited

Revision No. 1/2024 dated 16/7/67