5.4 Cybersecurity and Information Technology Policy

The company prioritizes and recognizes the importance of managing risks, maintaining cybersecurity and information technology systems to prevent risk levels and prepare for threats. The Risk Management and Monitoring Committee and a technical issue consideration team have been appointed.

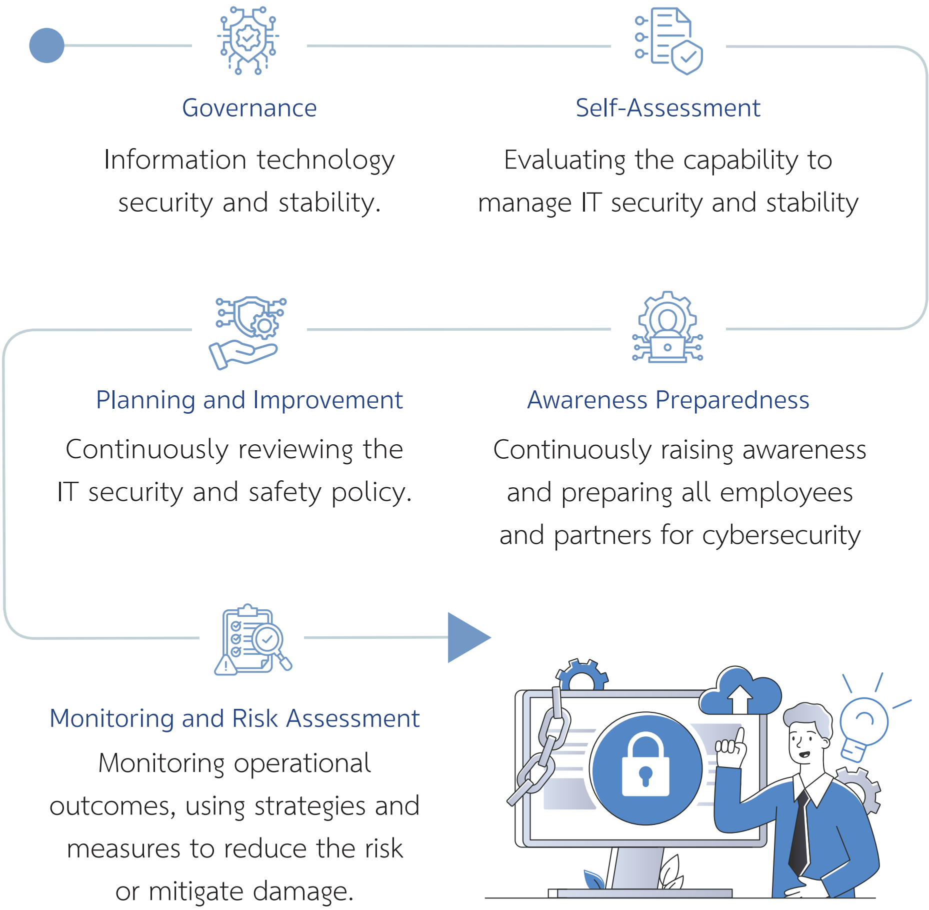
The company assesses its Cybersecurity Maturity based on the National Institute of Standards and Technology (NIST) framework to ensure confidence and security for customers and stakeholders comprehensively.

Actions are driven to align with the cybersecurity and information technology policy, which must be strictly complied.

Guidelines for managing risks to data security and information systems

The company has established guidelines for managing and administering the security of data and information systems that are in line with international standards such as ISO 27001 and the NIST Cybersecurity Framework. These guidelines offer principles and practices for risk management to enhance security and enable the company to plan, prevent, detect, and respond to threats swiftly, systematically, and effectively. The approaches are as follows:

The company has established systematic and effective guidelines for managing and controlling risks related to data and information system security. These guidelines are based on principles and practices that align with international standards, such as ISO 27001 and the NIST Cybersecurity Framework. The objective is to strengthen the security of data and IT systems to be robust and ready for planning, preventing, detecting, and responding to potential threats in a timely, systematic, and effective manner. The company operates according to the following guidelines.



Governance

Information technology security and stability.

Self-Assessment

Evaluating the capability to manage IT security and stability

Planning and Improvement

Continuously reviewing the IT security and safety policy.

Awareness Preparedness

Continuously raising awareness and preparing all employees and partners for cybersecurity

Monitoring and Risk Assessment

Monitoring operational outcomes, using strategies and measures to reduce the risk or mitigate damage.

Governance of Information Technology Security and Safety

In 2024, the company announced a policy on technology security and safety, taking into consideration significant legal requirements and stakeholder needs to define direction, principles, and a framework for operations. A committee was established, consisting of senior management and a working group on technology security and safety, to support resources, consider critical issues, and clearly assign responsibilities. The Information Technology department acts as the main unit, and the document can be downloaded at [website link].

https://www.satpcl.co.th/storage/content/sd/disclosure-documents/20230328-sat-policy-cyber-security-and-it-systems-th.pdf

Self-understanding through the assessment of capabilities in managing information technology security and safety.

The company participated in the Thai Stock Exchange’s (Cyber Resilience Survey 2023) for listed company groups in 2023, conducting assessments for major clients using the NIST Cybersecurity Framework Version 1 and Version 2. This allowed the company to understand its capabilities in managing information technology security and safety, enabling policy adjustments, planning, and continuous improvements to remain a leader among peers in the same industry, under appropriate resource investment.

Planning and improving information technology security policies

The company plans to control and oversee the information technology system, along with improving processes related to information technology security and data protection. This includes data analysis enhancement and extending the scope to cover all companies in the group, including subsidiaries, to ensure that the systems meet the appropriate standards. The preventive plans are as follows

Improvement

Review the Business Continuity Plan (BCP).

Supply Chain Risk Management

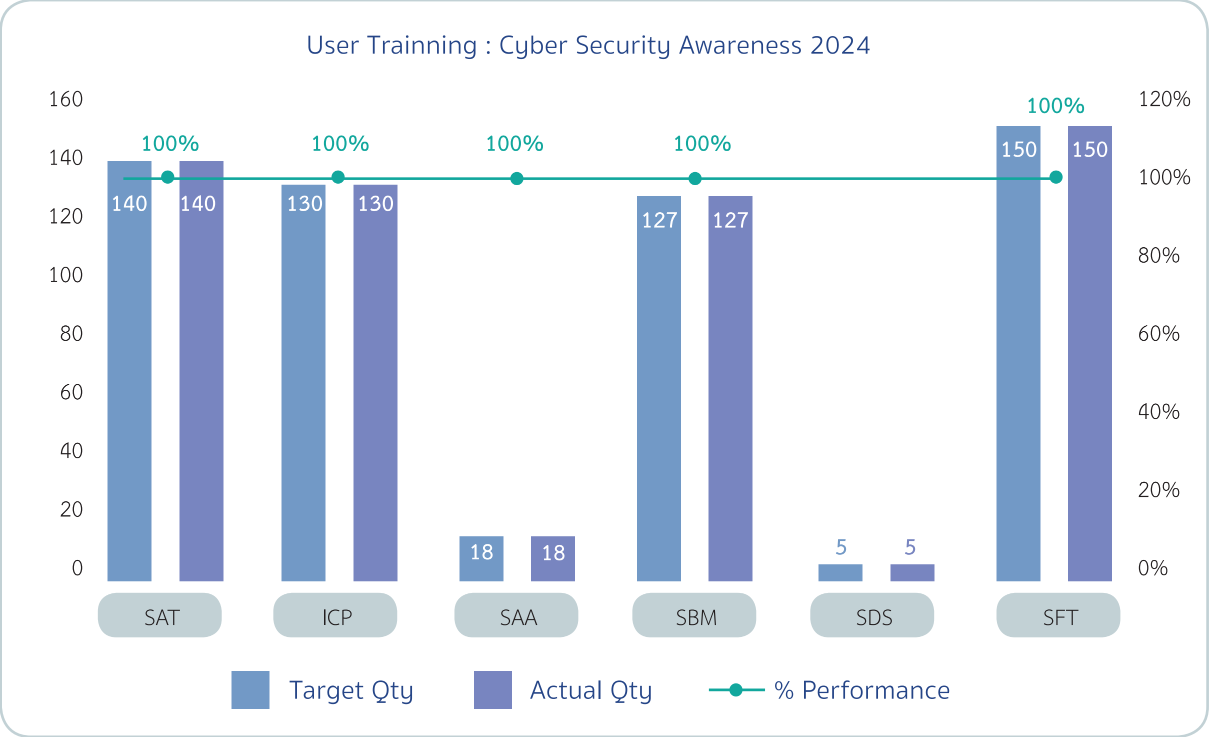
Conduct joint BCP drills with relevant partners.

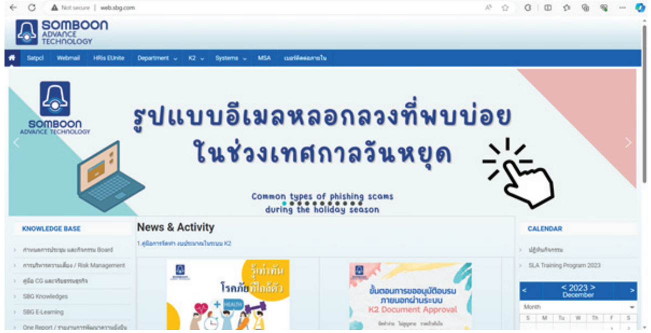
Analysis

Improve procedures for analyzing cybersecurity incidents upon receiving alerts.

Promoting awareness of the information technology security policy

The company organizes training sessions on cyber security and IT Policy for new employees and regular staff to foster awareness of data access and caution in data usage. Understanding is tested through self-learning systems and informational materials for employees at all levels.


User Trainning : Cyber Security Awareness 2024



รูปแบบอีเมลหลอกลวงที่พบบ่อย
ในช่วงเทศกาลวันหยุด

Common types of phishing scams
during the holiday season

KNOWLEDGE BASE
- กำหนดการประชุม และกิจกรรม Board
- การบริหารความเสี่ยง / Risk Management
- คู่มือ CG และจริยธรรมธุรกิจ
- SBG Knowledges
- SBG E-Learning
- One Report / รายงานการพัฒนาความยั่งยืน

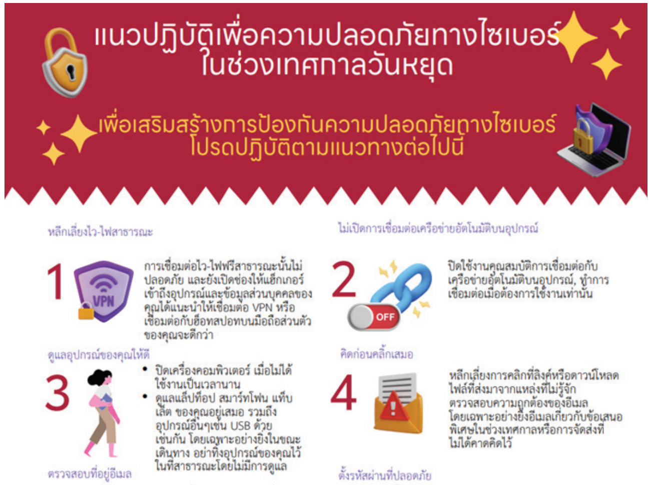
News & Activity
1.คู่มือการจัดทำ งบประมาณในระบบ K2

รู้เท่าทัน โรคภัยที่ใกล้ตัว

ขั้นตอนการขออนุมัติอบรมภายนอกผ่านระบบ K2 Document Approval

CALENDAR
- ปฏิทินกิจกรรม
- SLA Training Program 2023

< 2023 > December



แนวปฏิบัติเพื่อความปลอดภัยทางไซเบอร์
ในช่วงเทศกาลวันหยุด

เพื่อเสริมสร้างการป้องกันความปลอดภัยทางไซเบอร์
โปรดปฏิบัติตามแนวทางต่อไปนี้

หลีกเลี่ยงไว-ไฟสาธารณะ

1 การเชื่อมต่อไว-ไฟฟรีสาธารณะนั้นไม่ปลอดภัย และยังเปิดช่องให้แฮ็กเกอร์เข้าถึงอุปกรณ์และข้อมูลส่วนบุคคลของคุณได้แนะนำให้เชื่อมต่อ VPN หรือเชื่อมต่อกับฮ็อทสปอทบนมือถือส่วนตัวของคุณจะดีกว่า

ไม่เปิดการเชื่อมต่อเครือข่ายอัตโนมัติบนอุปกรณ์

2 ปิดใช้งานคุณสมบัติการเชื่อมต่อกับเครือข่ายอัตโนมัติบนอุปกรณ์, ทำการเชื่อมต่อเมื่อต้องการใช้งานเท่านั้น

ดูแลอุปกรณ์ของคุณให้ดี

3
- ปิดเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งานเป็นเวลานาน
- ดูแลแล็ปท็อป สมาร์ทโฟน แท็บเล็ต ของคุณอยู่เสมอ รวมถึงอุปกรณ์อื่นๆเช่น USB ด้วยเช่นกัน โดยเฉพาะอย่างยิ่งในขณะเดินทาง อย่าทิ้งอุปกรณ์ของคุณไว้ในที่สาธารณะโดยไม่มีการดูแล

คิดก่อนคลิ๊กเสมอ

4 หลีกเลี่ยงการคลิกที่ลิงค์หรือดาวน์โหลดไฟล์ที่ส่งมาจากแหล่งที่ไม่รู้จัก ตรวจสอบความถูกต้องของอีเมล โดยเฉพาะอย่างยิ่งอีเมลเกี่ยวกับข้อเสนอพิเศษในช่วงเทศกาลหรือการจัดส่งที่ไม่ได้คาดคิดไว้

ตรวจสอบที่อยู่อีเมล

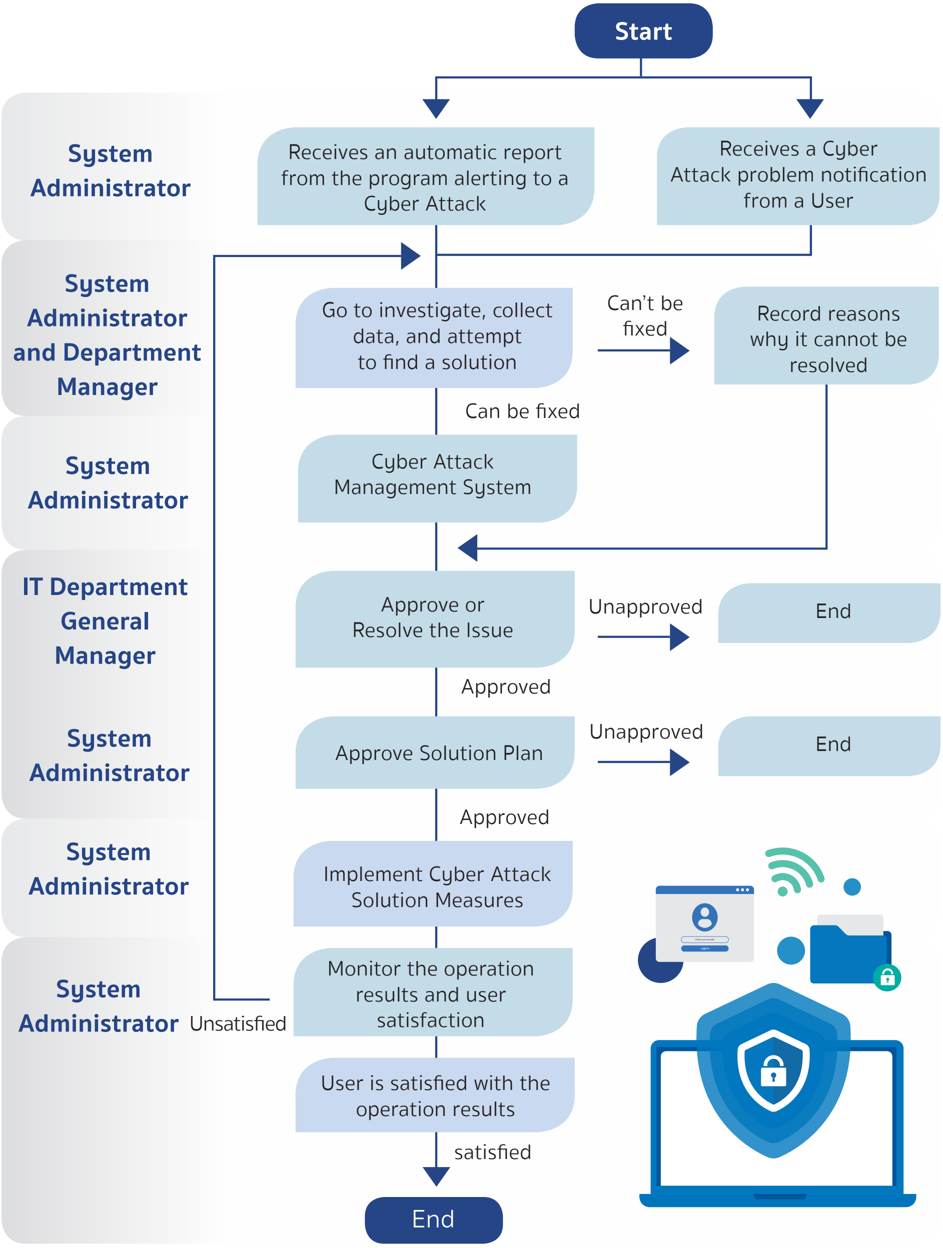
ตั้งรหัสผ่านที่ปลอดภัย

Continuous monitoring and risk assessment

Currently, the Information Technology department has conducted risk assessments with key risk indicators for evaluation, reporting to the organization-level risk committee monthly. This ensures effective risk management and minimizes potential impacts on the organization and business opportunities

Handling Complaints and Responding to Cybersecurity and Information Technology Incidents

The company has established a system for managing complaints regarding information technology security, accessible through a web application, email, and telephone. Employees can contact the complaint recipient around the clock via telephone or email through the Helpdesk system, an internal company web application, or at cybersecurity@somboon.co.th. The key steps include:


Start
System Administrator
Receives an automatic report from the program alerting to a Cyber Attack
Receives a Cyber Attack problem notification from a User
System Administrator and Department Manager
Go to investigate, collect data, and attempt to find a solution
Can't be fixed
Record reasons why it cannot be resolved
Can be fixed
System Administrator
Cyber Attack Management System
IT Department General Manager
Approve or Resolve the Issue
Unapproved
End
Approved
System Administrator
Approve Solution Plan
Unapproved
End
Approved
System Administrator
Implement Cyber Attack Solution Measures
System Administrator
Unsatisfied
Monitor the operation results and user satisfaction
User is satisfied with the operation results
satisfied
End

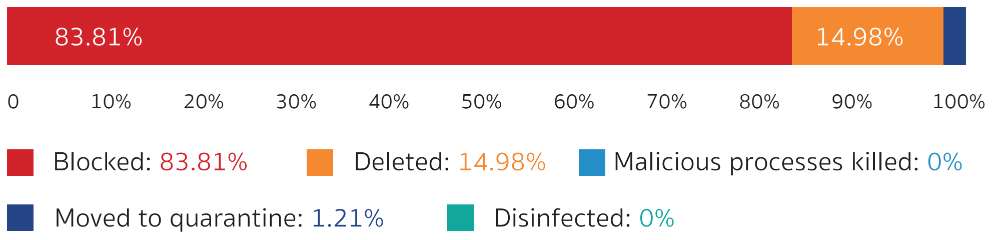
Performance Result of IT and Data Security in 2024

The Organization’s Preventive Computer Virus Capability for 2024

November			
Month	No of Attacks	No of Preventions	No of Successful Incidents
January	561	561	0
February	563	563	0
March	613	613	0
April	557	557	0
May	597	597	0
June	631	631	0
July	701	701	0
August	596	596	0
September	641	641	0
October	639	639	0
November	630	630	0
December	817	817	0
Total	7546	7546	0

Protection Model

Remediation actions



Performance 2024

1 Project to Upgrade ERP-SAP ECC to ERP-SAP S/4HANA

2 Establish a backup server system that provides authentication and authorization services for devices accessing the internal network in the Cloud

3 Prevented 100% of attacks from computer viruses

4 None of interrupted business continuity incidents arising from cybersecurity risk

5 The SAP-ERP system vulnerability test has been validated by an independent audit company.

6 Provided 100% of cybersecurity and information system trainings to new employees using computers.