# Cybersecurity Annual Report 2024

## Personnel

1. Monthly reports on the statistics of various types of cyber threats are regularly submitted to the Executive Committee and department managers.

2. Educational materials and cybersecurity awareness campaigns are disseminated through various channels to provide knowledge and preparedness against different types of threats. Informative emails are sent to all employees and executives every month.

3. Cyberattack simulation exercises are conducted to assess understanding and awareness of handling phishing emails.

4. The cybersecurity team is regularly sent to attend training and seminars to maintain up-to-date knowledge and skills.

## Process

| Category | Assessment Scores (1.0 5.0) |
|---|---|
| Assessment by Cybersecurity Resilience Survey by SET | 3.38 |

## Technology and Improvements Based on the NIST Cybersecurity Framework

The company has conducted a cybersecurity risk assessment in accordance with the NIST Cybersecurity Framework and has taken actions to enhance and strengthen its cybersecurity posture as follows:

| No. | Process | Information and Cybersecurity Control Projects |
|---|---|---|
| 1 | Identify | The company assesses its information technology security systems across various areas and implements activities to reduce associated risks. These areas include data protection against malware and viruses, cyberattacks, system failures, and threats posed by both internal and external personnel. In addition, the company continuously monitors and improves its cybersecurity systems, as well as adopt modern technologies to address emerging threats effectively. |

| | | |
|---|---|---|
| 2 | Protect | The company has enhanced its processes for accessing critical systems and allocated appropriate equipment that supports modern technologies suitable for current work practices. These improvements aim to increase security, reduce the risk of data breaches, and ensure compliance with the Personal Data Protection Act B.E. 2562 (2019). The key initiatives include:<br>• Assessing the capabilities of technologies used in securing access to high-critical systems<br>• Revising the policy on data classification levels<br>• Communicating and establishing guidelines for managing organizational and personal data |
| 3 | Detect | The company has upgraded its Security Operation Center (SOC) by enhancing monitoring, data collection, and analysis of security incidents. SOC operates on centralized data-driven technology and is supported by a dedicated team that provides 24/7 surveillance to ensure continuous cybersecurity protection. |
| 4 | Respond | The company continuously prepares for abnormal or emergency situations by conducting regular incident response drills and simulations of critical IT system attacks, including ransomware and personal data breaches. Additionally, phishing simulation tests are conducted to assess employees' awareness and response to fraudulent emails. |
| 5 | Recover | The company provides a test of Backup & Recovery system data recovery once a year and can recover as targeted. |