6.3 IT Security/ Cybersecurity Management

In order to strengthen information security protection and management mechanisms as well as comply with the Guidelines for Public Companies to Establish Internal Control Systems, our company passed the new Information Security Control Measures in a board meeting in 2022 and established an information security promotion organization to enhance risk control for information security. This organization is responsible for promoting, coordinating, supervising and reviewing matters concerning the management of information security, and the information security manager reports on the status of affairs to the board of directors annually. The annual information security policy and goals are approved by executives at or above the general manager level, and the policies and goals are reviewed regularly and effectively communicated to employees.

Our company has formed an information task force and recruited relevant professionals to join. In 2022, in addition to completing the SAP server drill and implementing the anti-hacking measures listed below, we invested in at least five IT personnel and spent Tens of millions of NT dollars on upgrading ERP software and hardware equipment. We also commissioned a professional vendor that complies with ISO 27001: Information Security Management System to plan, implement, maintain, manage and support our company's information system operations. Regarding education and training, the IT security task force conducted two Social Engineering Information Security Education and Training sessions for 185 employees, with an attendance rate of 71.71%; professional lecturers with abundant experience in information security service from a Taiwanese company were invited for the first time. We aim to strengthen employee awareness of information security and ensure that our company's information security management is recognized by employees through their feedback.

IT Secueraty

- Added "Information Security Control Measures" and established the Information
- The information security management system ISO 27001 will be implemented in 2024

Privacy Protection

- Strictly follow the EU General Data Protection Regulation (GDPR)
- Regarding the privacy and personal data security of patients and employees, we adhere to relevant policies and legal regulations to ensure their rights and interests are protected

Information Security Action Plan

Our company's information task force and hardware equipment have been gradually established and improved. In the future, we will continue to implement our Information Security Control Measures to ensure the appropriateness and effectiveness of our information security operations, regularly track and improve them, and establish a positive PDCA cycle.

We also plan to introduce ISO 27001: Information Security Management System in 2024, establishing an effective information security management mechanism to enhance everyone's awareness of information security.

Cybersecurity Measures of PharmaEssentia

- ✓ Strengthening of important core information system backups
- ✓ Drafting of information security policies (compliance with the GreTai Securities Market Information Security Management Control Guidelines)
- ✓ Planning and execution of information security checkups (annual execution)
- ✓ Planning and execution of employee social engineering training (annual execution)
- ✓ Information system and network vulnerability scanning (annual execution within the company)
- ✓ Information system and network penetration testing (annual execution from outside the company)
- ✓ Planning and implementation of file encryption systems
- ✓ Data loss prevention (DLP) endpoint device security protection
- ✓ O365 multi-factor authentication (MFA) for enhanced information security

Ensuring the Protection of Personal Privacy GRI418-1

The privacy policy of PharmaEssentia focuses on protecting personal information, including that of patients, healthcare professionals and other individuals involved in business transactions. Privacy protection is divided into two stages: clinical trial and drug launch. All of our partner research institution and hospitals for clinical trials are required to strictly follow our internal policy and national regulations, such as the General Data Protection Regulation (GDPR) in the European Union, Good Clinical Practice (GCP), the Helsinki Declaration and Taiwan's guidelines on ethical human research to ensure the protection of personal data. In 2022, there were no complaints of privacy violations or loss of customer data.

Global Cybersecurity Strategy – US Cybersecurity Column

Governance Responsibility

- Hired an IT Director with over 20 years of IT management experience as the highest information and network security executive, reporting directly to the VP of Business Operations
- Senior Operations Manager applied for the Certified Information Security Manager (CISM) certification
- Planning to establish relevant management processes and operating procedures before March 2023

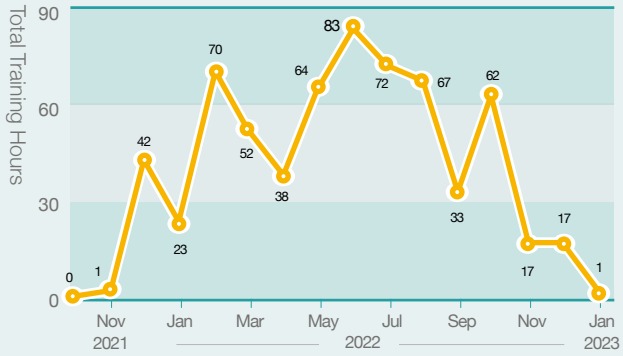
Risk Prevention

- The KnowBe4 system has an alert function. If an employee detects any abnormality, they can report it through the system and block potential phishing emails. If an employee feels that their account is at risk of information security, they can immediately seek IT support.
- Entrusted a third-party information security monitoring company to conduct IT audit management to prevent hackers or phishing attacks and collaborate to gradually improve management, including the establishment of more comprehensive policy and management processes, such as Bring Your Own Device (BYOD) Policy, Acceptable Use Policy, Asset Management, Security and Privacy Management Policy, IT Change Management Workflow, etc.
- No information security or network attacks have occurred to date.

Management Measures

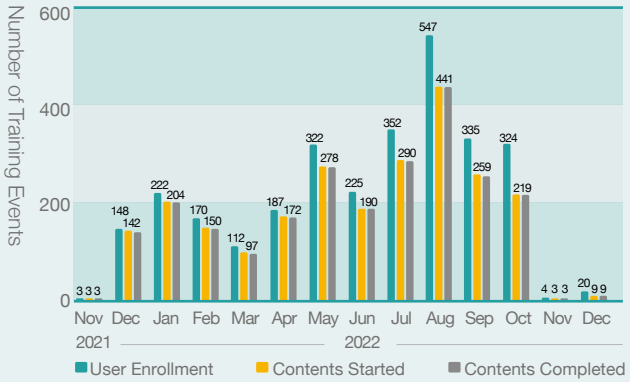
- Management Procedures: There is currently an internal operating procedure (SOP-IT-001) that not only manages information security risks but also provides management instructions for other events that may pose risks to the company's continuous operation.
- Education and Training: All employees receive policy and management procedure instructions to promote the importance of information security. Regarding the use of the KnowBe4 system, all employees are required to complete relevant training courses regularly. A total of 599 training hours were conducted in 2022.

Training Hours



This Report displays the number of hours selected users have spent training. Training hours includes any time spent on an assignment, regardless of completion status.

All Training Activities



This report displays a count of training events, grouped by month.