WHA GROUP

Policy

นโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

(Cybersecurity and Information Security Management Policy)

Cybersecurity Governance and Objectives

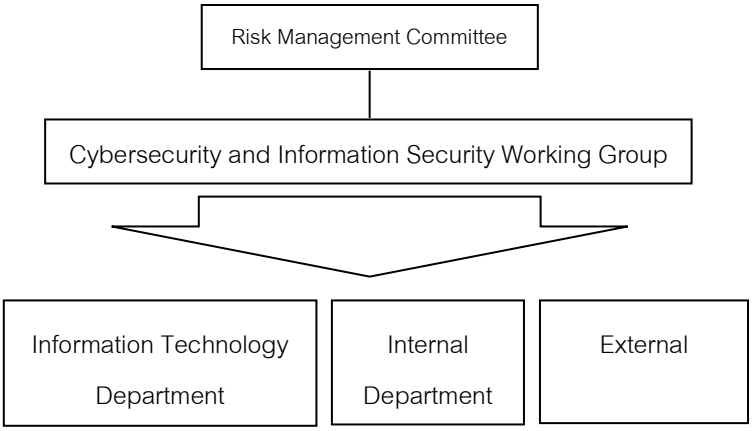
Objectives

- To provided employees to awareness and protection of cybersecurity and information security related to business operations of the organization.
- To compliance and focuses on Cyber Security Act of Thailand B.E. 2562 (2019), Personal Data Protection Act. (“PDPA”) and the revised version or other applicable laws/regulations in Thailand.

Cybersecurity Governance

The company has conducted information security management that complies with ISO/IEC 27001:2013 and the cybersecurity framework developed by National Institute of Standards and Technology of the United States of America (National Institute of Standards and Technology: NIST) and approved by the management. It is promulgated and implemented throughout the organization to be effective for personnel in all levels of the organization from executives, employees, as well as third parties involved in the use of information and assets, information of the organization.

In order to manage information security in a systematic and clear manner from management level to operational level The organization therefore has established a cyber and information security structure including role assignments and duties in the management of information security within the organization structure of the Cybersecurity and Information Security Working Group shown as the picture below.



Organizational structure of the Cybersecurity and Information Security Working Group

Board of Directors, working groups or related agencies	Roles and Responsibilities
Risk Management Committee	- Establish policies and framework for corporate risk management. - Set strategic direction and goals
Cybersecurity and Information Security Working Group	- Review and approve the improvement of the information security policy as scheduled or according to the situation.

	- Make a public relations plan and training in every unit to understand information security - Review and approve projects related to information security. - Plan, monitor and manage various risks arising from system constraints. - Review, review and assess the Security Continuity Plan in case of emergency.
- Information Technology Department	- Define systems, practices and services for users to follow cybersecurity and information security policy - Assessing performance monitoring and reporting risks to the Enterprise Risk Management Committee
- Internal Department	- Provide support in accordance with the Cybersecurity and Information Security Management Policy. - Follow the cybersecurity and information security policy.
- External	- Follow the cybersecurity and information security policy.

Company has appointed Vice President of Information Technology Department to hold Chairman of the Cybersecurity and Information Security Working Group as Chief Information Security Officer (CISO) with the following duties:

(1) To be the chairman of the Cybersecurity and Information Security Working Group; and is responsible for information security and is the leader in all operations related to information security in the organization.

(2) Set goals Information security policy to be in line with the strategic plan of the organization.

(3) To be the presenter of the operational plan, policy, budget, manpower, as well as an information security operation plan for approval from the senior management. and to make senior management aware of the importance of information security

(4) Analyze and manage risks related to information security. as well as assessing options for dealing with IT security risks appropriately.

(5) Manage the development of information security policies. In order for the organization to obtain confidentiality, integrity and availability of information.

<u>Guidelines and processes for information security and cybersecurity management according to ISO/IEC 27001:2013 standard</u>

1) INFORMATION SECURITY
2) ORGANIZATION OF INFORMATION SECURITY
3) HUMAN RESOURCES SECURITY
4) ASSET MANAGEMENT
5) ACCESS CONTROL
6) CRYPTOGRAPHY
7) PHYSICAL AND ENVIRONMENTAL SECURITY

8) OPERATIONS SECURITY

9) COMMUNICATIONS SECURITY

10) SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

11) SUPPLIER RELATIONSHIPS

12) INFORMATION SECURITY INCIDENT MANAGEMENT

13) INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

14) COMPLIANCE

- END OF DOCUMENT -