WHA GROUP

Policy

Cybersecurity, Information Security & Privacy and AI Governance Policy

Cybersecurity, Information Security & Privacy and AI Governance Policy

WHA Group recognizes the importance of information technology and Artificial Intelligence (AI) as key mechanisms for enhancing the efficiency and effectiveness of organizational operations, supporting the pursuit of business excellence, and driving the organization in the digital era. These technologies contribute to innovation, sustainable value creation for stakeholders, and long-term organizational growth. WHA Group is firmly committed to protecting and securing data and information systems, as well as to the use, development, and application of AI under the principles of security, good governance, fairness, transparency, and accountability.

Therefore, WHA Group has established this Cybersecurity, Information Security & Privacy and AI Governance Policy, based on compliance with applicable laws, regulations, practices, and international standards, to ensure that the use and management of such technologies are systematic, secure, transparent, and trustworthy.

1. Policy Objectives

1.1 **To build trust and maintain cybersecurity and information security** by protecting the organization's information and information systems to ensure confidentiality, integrity, and availability in accordance with ISO/IEC 27001.

1.2 **To protect personal rights and personal data** by establishing transparent personal data management foundations in alignment with ISO/IEC 27701.

1.3 **To develop and apply artificial intelligence ethically** by establishing a framework for AI development and use that is responsible, transparent, unbiased and fair, together with maintaining data security and privacy, and establishing an auditable governance system, in order to reduce potential risks to humans and society in accordance with ISO/IEC 42001.

1.4 **To comply with laws, regulations, standards, and international practices** by focusing on operations that comply with applicable laws, regulations, business contractual obligations, and other relevant international standards and practices.

2. Definitions

2.1 "WHA Group" or "Organization" means WHA Corporation Public Company Limited and its subsidiaries, including affiliated companies in which the Company has the power to control, direct, and lay down policies.

2.2 "Policy" means this Cybersecurity, Information Security & Privacy and AI Governance Policy, including any amendments, as well as any other policies, procedures, guidelines, or operating standards related to cybersecurity, information security, privacy, and AI governance established by WHA Group and approved by the Group Chief Executive Officer and/or the Chief Executive Officer of the subsidiary that has signed and promulgated such documents.

2.3 "Guidelines" means practices relating to the management of cybersecurity, information security, privacy, and Artificial Intelligence (AI) governance established and announced by WHA Group for users to strictly comply with.

2.4 "Entities under the organization's management authority" means entities that the organization can control and direct, whether through shareholding with voting rights exceeding 50 percent or through control of the majority of voting rights at shareholders' meetings. Such management authority includes decision-making and oversight of operations, as well as shared use of information technology systems, networks and computers, and Artificial Intelligence (AI) technologies.

2.5 "Supply Chain" means the network of relationships among the organization, its business partners, contractors of such partners, and other parties involved in the management of cybersecurity, information security, privacy, and Artificial Intelligence (AI) governance of the organization and related entities under the organization's management authority.

2.6 "Information" means data, news, records, history, document text, computer programs, computer data, images, sounds, marks, and symbols, whether stored in a form that can be directly understood by a person or through a computer or any other means that allows the recorded matter to be displayed.

2.7 "Information System" means a system that collects, stores, processes, and distributes data to produce useful information for decision-making and operations of individuals or organizations. The system comprises key components such as hardware, software, data, people, processes, and networks. Its primary function is to transform raw data into meaningful information to support management and achievement of organizational objectives.

2.8 "Information Technology" means technology used in business operations, covering data or information, operating systems, application systems, database systems, computer and network equipment, and communication networks, among others.

2.9 "Information Technology Security" means the protection of information systems and data to ensure confidentiality, integrity, and availability at all times, preventing unauthorized access, alteration, or destruction of data through administrative, technical, and physical measures to address various threats.

2.10 "Cyber" means data and communications arising from services or applications using computer networks, the Internet, telecommunications networks, ordinary satellite services, and similar interconnected network systems in general.

2.11 "Cybersecurity" means measures or actions established to prevent, respond to, and reduce risks from all forms of cyber threats, whether internal or external, that may affect the organization's business operations, national security, economic security, military security, or public order.

2.12 "Cyber Threat" means any unlawful act or operation using a computer, computer system, or malicious program with the intent to cause damage or abnormality to a computer system, computer data, or other related data, and which poses danger affecting the operation of computers, computer systems, or related data.

2.13 "Artificial Intelligence (AI)" means technology developed to enable computer processing systems, robots, machines, or electronic devices to exhibit characteristics or behaviors similar to humans according to objectives defined by humans, such as learning, perceiving and responding to the environment, reasoning, and problem-solving.

3. Scope of the Policy

3.1 This Policy applies to the Board of Directors, executives, employees, and personnel at all levels of WHA Group, as well as entities under the organization's management authority. It covers all information assets and systems of the organization, including information technology systems, data and digital assets, devices, and any systems connected to or accessing the organization's network, regardless of location, time, or mode of use.

3.2 This Policy covers external parties, business partners, contractors, service providers, and stakeholders who are authorized to access or use WHA Group's information systems, information, personal data, information technology assets, AI systems, or any services. The organization is committed to applying the principles under this Policy to such persons through the Supplier Code of Conduct, contractual requirements, service level agreements, terms and conditions of service, or other practices as appropriate.

3.3 In the event that any announcements, rules, orders, or other organizational practices conflict with this Policy, this Policy shall prevail.

4. Governance Structure and Key Policy Practices

4.1 To ensure effective management, WHA Group defines the hierarchy of governance documents as follows:

4.1.1 **Master Policy** means this Policy, which defines the direction, core vision, and fundamental principles of the organization's operations, serving as the main conceptual framework for decision-making and the establishment of procedures at subsequent levels.

4.1.2 **Standards** means technical requirements and minimum criteria that must be strictly followed to ensure operations comply with standards established by WHA Group, such as the Cybersecurity and Information Security Management Standard or the AI Management Standard.

4.1.3 **Procedures and Guidelines** means detailed work instructions and operational guidance that enable personnel to correctly and consistently apply policies and standards in actual operations.

4.2 To ensure compliance with this Policy, WHA Group shall prepare, establish, and/or review measures, standards, and operational policy guidelines in the following areas:

4.2.1 Privacy Policy

4.2.2 Cybersecurity and Information Security Management Standard

4.2.3 AI Management Standard

4.2.4 Other relevant and necessary standards, measures, manuals, procedures, or guidelines.

4.3 WHA Group shall regularly review and update measures to align with applicable laws, regulations, and government requirements relating to cybersecurity, personal data, and information technology.

4.4 Any relevant guidelines prepared and/or announced prior to the date of this Policy shall be deemed guidelines issued under Clause 4 of this Policy.

5. Roles, Duties, and Responsibilities

5.1 The Risk Management and Information Security Committee shall be responsible for overseeing operations to ensure compliance with this Policy.

5.2 This Policy shall be reviewed at least once a year or whenever there are significant changes in applicable laws, technology, or relevant threats, to ensure that the principles of this Policy remain aligned with the organization's context and business environment at that time.

5.3 The Group Chief Executive Officer, the Chief Executive Officer of each subsidiary, the Chief Technology Officer, and/or the Chief Legal Officer shall have the authority to consider, review, and approve standards and relevant guidelines issued under this Policy.

5.4 All employees and personnel of WHA Group are responsible for immediately reporting abnormal cyber events, data leakage, or inappropriate AI use to the Information Security Team or Incident Response Team (IRT) upon discovery. If the leaked data constitutes personal data, the incident must also be reported to the Data Protection Officer (DPO) at the same time, so that it can enter the incident response process in accordance with the defined standards.

6. Audit and Compliance

WHA Group reserves the right to audit the use of information systems, data, and AI to the extent permitted by law, to ensure that operations comply with this Policy and to prevent potential threats.

7. **Awareness and Training**

   WHA Group shall provide training and knowledge assessments on Cybersecurity, Privacy, and AI Ethics for employees and relevant parties at least once a year to ensure that everyone understands and is aware of their responsibilities.

8. **Penalties**

   Any violation, breach, or failure to comply with this Policy or related guidelines shall be considered a disciplinary offense and shall be subject to disciplinary action in accordance with WHA Group's work rules. If such act causes damage or constitutes a legal offense, WHA Group shall pursue civil and criminal proceedings against the offender.

This Cybersecurity, Information Security & Privacy and AI Governance Policy was reviewed and endorsed by the Risk Management and Information Security Committee at Meeting No. 3/2026 held on July 23, 2026, and was reviewed and approved by the Board of Directors at Board Meeting No. 5/2026 held on August 10, 2026.

-Somkid Jatusripitak-

(Mr. Somkid Jatusripitak)

Chairman of the Board of Directors

WHA Corporation Public Company Limited