Sino-Ocean Group Information Security Policy

Sino-Ocean Group strictly complies with laws and regulations related to information security, formulates and continuously improves its information security policies to comprehensively prevent risks associated with information security and data privacy, and effectively safeguards the legitimate rights and interests of employees, clients, partners, and other stakeholders. This policy aims to standardize behaviors within the Group and with external parties regarding information handling, system access, and data protection. It requires directors, all employees (including non-permanent staff), and all third parties with business relationships with the Group to fully understand and strictly adhere to relevant principles and regulations on information security, working together to build a secure, trustworthy, and sustainable information ecosystem.

The Sustainable Development Management Committee, authorized by the Board of Directors, is responsible for comprehensive ESG management. The Group has established an Information Security Management Committee, and the deputy general manager of the President's Office Center serves as the head of the committee, responsible for overseeing information security issues and reporting annually on the information security management to senior management. This policy is approved by the Sustainable Development Management Committee authorized by the Board of Directors.

The Company commits to:

- Continuously improving information security systems, developing and refining information security-related business continuity plans to ensure integrity and protection of data;

- Proactively monitoring and responding to information security threats, enhancing incident response mechanisms and procedures, and regularly conducting independent external audit of the IT infrastructure or information security management systems and information security vulnerability analysis to continuously strengthen its capability in managing information security risks;

- Establishing and refining escalation process for employees to report incidents, vulnerabilities or suspicious activities, clearly defining individual responsibilities for information security for the entire workforce, ensuring that each employee understands their role and obligations in information protection. Any violation of this policy or other related information security regulations will be subject to

disciplinary actions, including warnings or other sanctions, depending on the severity of the offense;

- Conducting regular information security awareness training to enhance employees' awareness and protective capabilities;

- Establishing information security requirements for third parties (e.g., suppliers) to ensure compliance with the Group's information security policies and practices.

This policy is updated every three years. It can be reviewed and updated as appropriate when necessary.