China Hongqiao Group Limited
中国宏桥集团有限公司
(Incorporated in the Cayman Islands with limited liability)
(the "Company")
(Stock Code: 1378)

INFORMATION SECURITY POLICY

(Adopted by the Sustainability Committee of the Company on 24 April 2026)

I. Core Concepts and Objectives

China Hongqiao Group Limited (hereinafter referred to as "China Hongqiao" or "the Group") deeply recognises the strategic value of information assets in the digital era. The Group is committed to building an information security governance system featuring holistic coordination and defence-in-depth, deeply integrating an information security culture into the entire process of business operations, and systematically protecting the information assets of the Group and stakeholders, thereby establishing a robust information security barrier for its long-term development. This policy is hereby formulated to guide and regulate the Group's information security management, continuously enhance its information security protection capabilities, and ensure business compliance and robust operations.

II. Scope of Application

This policy applies to all employees of China Hongqiao Group and its subsidiaries/branches (full-time employees, part-time employees, interns, and dispatched workers, including board members and senior management), covering all aspects of the entire value chain such as research and development (R&D), procurement, production, operations, sales, and services.

III. Commitments and Practices

1. Information Security Compliance

The Group strictly complies with applicable information security laws, regulations, and regulatory requirements of the countries or regions in which it operates, and implements information security management measures in accordance with relevant rules and requirements. In addition, the Group has established the Supplier Code of Conduct to specify information security management requirements applicable to third parties (including, but not limited to suppliers).

2. Information Security Management

The Group establishes and continuously improves its information security management system, thereby building an information security management structure with clearly defined responsibilities. The Sustainability Committee under the Board of Directors holds supervisory responsibility for the implementation of information security strategies and objectives. The Digital Intelligence Management Department is responsible for coordinating, guiding, and managing information security efforts. The Group continuously optimises its information security management policies, deploys and implements information security management measures, and continuously improves information security systems and upgrades technical protection methods to protect all information assets of the Group and systematically prevent unauthorised access, tampering, disclosure, loss, destruction, or illegal use of data and information, thereby ensuring the integrity, confidentiality, and security of data and information. The Group regularly engages third-party organisations to conduct data security risk assessments, and continuously strengthens its capabilities for dynamic risk assessment, monitoring, and response. In addition, the Group evaluates the effectiveness of management measures through third-party testing, internal and/or external audits, identifies potential vulnerabilities, and continuously optimises control strategies based on regulatory changes, business requirements and other relevant factors, thereby ensuring the effectiveness and adaptability of data security management.

3. Information Security Incident Response

The Group has established a routine information security monitoring and emergency response mechanism, deploying monitoring tools to achieve real-time risk alerting and setting up an efficient, closed-loop emergency response process. This ensures timely reporting and prompt handling in the event of an information security incident, thereby avoiding or minimising the adverse impact of such emergencies on business operations. The Group has formulated an information security incident emergency response plan, specifying the procedures for handling information security incidents, and regularly organises emergency drills for information security incidents to continuously strengthen its response capabilities for information security emergencies and ensure rapid risk control and swift business recovery when incidents occur.

4. Information Security Education

The Group places great emphasis on information security education. Every employee is required to assume responsibility for the security protection of the Group’s information assets to which they have access, and shall strictly comply with this policy and the Group’s relevant information security rules and regulations. The Group attaches importance to information security education by conducting awareness campaigns and policy communications on information security basics for all employees. Through internal case studies, experience sharing, and security bulletins, the Group enhances the information security awareness of all employees. In addition, the Group provides enhanced training and education for personnel in information security-related roles, continuously strengthens their risk prevention capabilities, and actively fosters an information security culture involving all employees.

5. Supervision, Incentives, and Accountability

The Group has established a management mechanism that combines constraints and incentives to ensure the effective implementation of the information security policy. On the one hand, the Group shall impose accountability and disciplinary actions against responsible personnel for violations such as unauthorised disclosure of information or data, strictly in accordance with applicable regulations. On the other hand, the Group encourages all employees to proactively report information security risks or propose improvement suggestions. The Information Security Management Department shall timely handle and provide feedback, and shall give appropriate incentives to employees who make effective reports or positive contributions, thereby fostering a positive culture where "security is everyone’s responsibility".

IV. Supplementary Provisions

1. Continuous Improvement

The Group will, as necessary, revise this policy from time to time according to regulatory and legal changes, updates to industry standards and feedback from stakeholders, and publicly update the content through the official website, ESG reports/sustainability reports and other channels to ensure the continuous adaptability and effectiveness of the policy.

2. Approval Authority

The policy is reviewed and approved by the Sustainability Committee under the Group's Board of Directors and shall come into force on the date of issuance.

3. Interpretation

The policy shall be interpreted by China Hongqiao. The document is prepared in both Chinese and English. In case of any discrepancy between the Chinese and English versions, the Chinese version shall prevail.