HENDERSON LAND DEVELOPMENT COMPANY LIMITED
恒基兆業地產有限公司
Incorporated in Hong Kong with limited liability
(Stock Code : 12)

CYBERSECURITY POLICY

Purpose

Henderson Land Development Company Limited (the "Company") and its subsidiaries (collectively the "Group") are committed to continuously improving information security system through establishing, implementing and upholding standards for safeguarding information system. This Policy sets out the Group's commitment to ensuring integrity and data protection, ongoing enhancement of security measures, and strict adherence to best practices of cybersecurity, both internally and for third parties.

Governance

- The Board of Director, through the Audit Committee receiving pertinent updates on cybersecurity issues from Audit Department and Information Technology Department, provides oversight of the Group's cybersecurity strategy, encompassing the identification, monitoring, mitigation, and management of cyber risks.
- The Audit Committee works in close coordination with the Audit Department and Information Technology Department which conduct annual internal audit and oversee all aspects of information security, including the governance of information technology infrastructure, and requires the embedding of cybersecurity measures into the daily operations of all business units, thereby ensuring the effective execution of the Group's cybersecurity strategy.

Preventing, monitoring, and responding to information security threats

- To mitigate the risk of data breaches, Data Governance and Management Policy has been established and available internally, outlining the guiding principles and responsibilities of all employees in safeguarding data security throughout the entire data lifecycle. Additionally, Business Continuity Plan is in place to ensure the timely recovery of information systems and data in the event of cybersecurity incidents.
- Internal audits and disaster recovery drills are conducted semi-annually to evaluate and enhance the Group's ability to recover and maintain critical information systems during disaster scenarios.

July 2025

- External cybersecurity assessments and vulnerability analyses are performed periodically to identify potential risks and weaknesses in the Group's computer systems, applications, and network infrastructure. These proactive measures strengthen our overall cybersecurity posture and preparedness against emerging threats.
- A clearly defined escalation and incident response process has been implemented to promptly report, investigate, and address any suspected IT security incidents or data breaches. This ensures timely and effective corrective actions are taken to minimise risk and impact.

Communication

We have clearly established individual responsibilities on information security to ensure that all staff/ third-parties understand their roles in safeguarding the Group's assets, which includes:

- Internal Information Technology Policy for Henderson Group and Security Guidelines are available on the Group's Intranet to inform employees' responsibilities.
- A Third-party Management Guideline is available, which sets out the controls that must be taken to identify, assess and manage the risk with the services upon third-party.
- Regular training sessions on cybersecurity and data awareness are available for all staff.

Review of this Policy

The Company will review this Policy from time to time as appropriate, and in any event, once every three years.