新鴻基地產
Sun Hung Kai Properties

網絡安全政策

新鴻基地產發展有限公司（「新鴻基地產」）致力保障持份者免受網絡安全風險。

本政策適用於新鴻基地產及其附屬公司（統稱為「集團」）。集團業務單位應遵守本政策，並在適用的情況下，根據其業務性質訂立、檢討及更新其所屬政策。集團鼓勵聯營、合資公司、供應鏈的合作夥伴（包括供應商、承辦商及分判商）及其他服務供應商遵守本政策。本政策涵蓋以下範疇：

管治

- 董事局透過執行委員會負責監督集團的網絡安全策略，及識別、監察、減低和管理網絡安全風險。
- 集團的資訊科技管治督導委員會向執行委員會報告，並協助執行委員會監督集團的資訊安全，包括集團網絡基建安全。
- 資訊科技管治督導委員會亦協助執行委員會監察集團執行網絡安全策略，並與資訊科技部門密切合作，將網絡安全融入各業務單位的日常運作之中。

溝通

- 內部資訊科技政策及指引已上載至集團內聯網，告知員工其網絡安全責任。
- 定期開展數據隱私和信息安全培訓，提高員工的網絡安全風險意識。

合規

- 所有員工必須遵從本政策以及其他適用的資訊科技政策。如果出現嚴重違反本政策及其他適用的資訊科技政策的情況，集團將采取紀律處分。

監察及匯報

- 制定並採用網絡事件響應方案，明確集團處理網絡威脅和事件的程序、步驟和責任。集團每年對網絡事件影響方案的有效性進行測試。
- 進行外部網絡安全評估或漏洞分析，以識別及了解電腦系統、應用程式和網絡基礎設施中的漏洞及風險，提高集團抵禦網絡威脅的能力和準備。
- 為資訊科技基礎設施和信息安全管理系統進行內部和外部審核。
- 制定明確的事件升級流程，以及時處理可疑的資訊科技問題。
- 資訊科技管治督導委員會因應情況定期檢討本政策，確保本政策有效可行。

中英文版本如有歧異，應以英文版本為準。