



网络安全政策

新鸿基地产发展有限公司（“新鸿基地产”）致力保障持份者免受网络安全风险。

本政策适用于新鸿基地产及其附属公司（统称为“集团”）。集团业务单位应遵守本政策，并在适用的情况下，根据其业务性质订立、检讨及更新其所属政策。集团鼓励联营、合资公司、供应链的合作伙伴（包括供应商、承包商及分包商）及其他服务供应商遵守本政策。本政策涵盖以下范畴：

管治

- 董事局透过执行委员会负责监督集团的网络安全策略，及识别、监察、减低和管理网络安全风险。
- 集团的资讯科技管治督导委员会向执行委员会报告，并协助执行委员会监督集团的资讯安全，包括集团网络基建安全。
- 资讯科技管治督导委员会亦协助执行委员会监察集团执行网络安全策略，并与资讯科技部门密切合作，将网络安全融入各业务单位的日常运作之中。

沟通

- 内部资讯科技政策及指引已上载至集团内联网，告知员工其网络安全责任。
- 定期开展数据隐私和信息安全培训，提高员工的网络安全风险意识。

合规

- 所有员工必须遵从本政策以及其他适用的资讯科技政策。如果出现严重违反本政策及其他适用的资讯科技政策的情况，集团将采取纪律处分。

监察及汇报

- 制定并采用网络事件响应方案，明确集团处理网络威胁和事件的程序、步骤和责任。集团每年对网络事件影响方案的有效性进行测试。
- 进行外部网络安全评估或漏洞分析，以识别及了解电脑系统、应用程式和网络基础设施中的漏洞及风险，提高集团抵御网络威胁的能力和准备。
- 为资讯科技基础设施和信息安全管理系统进行内部和外部审核。
- 制定明确的事件升级流程，以及时处理可疑的资讯科技问题。
- 资讯科技管治督导委员会因应情况定期检讨本政策，确保本政策有效可行。

中英文版本如有歧异，应以英文版本为准。