新鴻基地產
Sun Hung Kai Properties

Cybersecurity Policy

Sun Hung Kai Properties Limited ("SHKP") is committed to safeguarding its stakeholders from cybersecurity risks.

This Policy is applicable to SHKP and its subsidiaries (collectively: the Group). Business units of the Group are expected to abide by this Policy. Where applicable, they will establish, review and update their own policy in accordance with their business nature. The Group's associated and joint venture companies, supply chain partners (including suppliers, contractors and subcontractors) and other service providers are encouraged to comply with this Policy. This Policy covers the following areas:

Governance

- The Board of Directors, through the Executive Committee, is responsible for overseeing the Group's cybersecurity strategy, and identifying, monitoring, mitigating and managing cybersecurity risks.
- The Group's IT Governance Steering Committee reports to the Executive Committee and assists the Executive Committee in overseeing the Group's information security, including the security of the Group's IT infrastructure.
- The IT Governance Steering Committee also assists the Executive Committee in overseeing the implementation of the Group's cybersecurity strategy and works closely with the IT Department to build security into the daily operations of every business unit, ensuring the integrity and protection of data, and the continuous improvement of information security systems.

Communication

- Internal IT Policies and Guidelines are uploaded to the Group's Intranet to inform employees of their cybersecurity responsibilities.
- Conduct regular data privacy and information security training to raise awareness of cybersecurity risks among employees.
- Establish individual responsibility for information security throughout the entire workforce, ensuring employees understand their roles in protecting the Group's information assets.

Compliance

- Employees are required to comply with this Policy and other applicable IT Policies. The Group may initiate disciplinary action in the case of serious violation of this Policy and other applicable IT Policies.
- Establish applicable requirements for third parties (e.g. suppliers) to ensure that they adhere to the Group's information security standards and practices.

Monitoring and Reporting

- Establish and adopt a cyber incident response plan that specifies the Group's procedures and responsibilities when handling cyber threats and incidents. In addition, the Group conducts testing on the effectiveness of the incident response plan annually.

- Perform external cybersecurity assessment or vulnerability analysis to identify vulnerabilities and risks in computer systems, applications and network infrastructures, so as to improve the Group's protection and preparedness against cyber threats.
- Conduct internal and external audits for the IT infrastructure and information security management systems.
- A clear escalation process is in place to address suspicious IT issues and problems.
- Review this policy by the IT Governance Steering Committee periodically for adequacy and effectiveness, as appropriate.

If there is any inconsistency or ambiguity between the English version and the Chinese version, the English version shall prevail.