新鴻基有限公司
SUN HUNG KAI & CO. LIMITED
*(Incorporated in Hong Kong with limited liability)*
**(Stock Code: 86)**

# Extract of Group Information Security Policy

Sun Hung Kai & Co. Ltd and its subsidiaries (the "**Group**") is committed to protecting our digital assets and ensuring the confidentiality, integrity, and availability of our information systems.

This Group Information Security Policy (the "**Policy**") aims to provide a comprehensive framework for protecting the Group's information assets while ensuring compliance with relevant laws, regulations, and standards. It also promotes awareness and training among employees to ensure that everyone understands their responsibilities and the importance of information security.

The Policy defines general framework on information security, which include but not limit to cybersecurity, disaster recovery plan, and data loss prevention.

## Cybersecurity

The cybersecurity related sections in the Policy establishes guidelines, procedures, and controls to protect the Group's information systems and data from cyber threats, such as hacking, malware, phishing, and other forms of cyber-attacks.

Cybersecurity includes measures for preventing, detecting, and responding to cyber threats, such as access controls, encryption, incident response, data backup and recovery, and employee training and awareness programs.

- Preventing
  The Group has implemented a number of security measures to proactively prevent cyber threats and attacks. This includes access controls, network security, encryption, patch management, security awareness training, and physical security. The objective is to reduce the risk of cyber threats and attacks and better protect the Group's information systems and data.

- Detecting
  The Group is also equipped with the latest cybersecurity technology for identifying and detecting cyber threats and attacks as early as possible. This includes measures such as network monitoring, intrusion detection and prevention systems, security information and event management (SIEM), dark web monitoring and vulnerability scanning. The objective is to quickly identify potential security incidents and take appropriate action to prevent or mitigate their impact. By implementing effective detecting measures, the Group can reduce the time it takes to respond to security incidents and limit the damage they can cause.

- Responding to Cyber Threats
  This relates to responding to security incidents and mitigating their impact, and includes measures such as incident reporting procedures and disaster recovery planning. The objective is to minimize the damage caused by security incidents and restore normal operations as quickly as possible. By implementing effective response measures, the Group can reduce the impact of security incidents and maintain the trust and confidence of our stakeholders.

The objective is to reduce the risk of cyber attacks, data breaches, and other security incidents that could result in financial losses, legal liabilities, damage to reputation, or other negative consequences for the Group. By implementing effective cybersecurity policies and procedures, the Group can better protect our information systems and data and ensure business continuity in the face of cyber threats.

## Disaster Recovery Plan (DRP)

The Disaster Recovery Plan outlines procedures for recovering systems and application services for the Group, with the objective of ensuring timely recovery of system operations to continue business operations. The plan provides the necessary organization, resources, and procedures to facilitate this recovery process.

## Data Loss Prevention

Data Loss Prevention related control in the Policy is to ensure that users are aware of any sensitive or restricted data they may be transferring and to safeguard the Group's reputation and customers from any adverse impact due to data loss.

*(This is an extract of the Policy and if there is any inconsistency and ambiguity between the English version and the Chinese version, the English version shall prevail.)*