

Information Security Policy

Poly Property Services Co., Ltd. (hereinafter referred to as “Poly Property” or the “Company”) attaches great importance to information security management. The Company is committed to safeguarding the security of its information systems, network equipment, data assets and relevant information storage media to prevent risks including unauthorised access, leakage, tampering, destruction, misrepresentation and malicious attacks, ensuring the continuity, stability and reliability of business operations for the Company.

This policy applies to Poly Property and its holding subsidiaries. All investee companies, suppliers, contractors and other business partners are encouraged to comply with this policy.

I. Governance Structure

- Establish an information security management mechanism, with relevant functional departments coordinating information security management to promote the development of information security systems, system security management, risk identification, issue collection, inspection, supervision, and implementation of rectification;
- Each business department and relevant unit should, according to their respective responsibilities, cooperate in carrying out information security management to promptly identify, report and address information security issues, thereby jointly safeguarding the security of information systems and data assets of the Company.

II. Specific Measures

- Continuously strengthen the operation and maintenance management of information systems and standardise management requirements for system accounts, passwords, logs, monitoring and backups, ensuring the safe and stable operation of information systems;
- Implement necessary management control over the development, change, deployment, testing, acceptance and maintenance of information

systems, including assessment, approval, backup and risk control during system development and change management to minimise the impact on business operations;

- Strengthen cybersecurity and terminal security management by performing necessary configuration, monitoring, maintenance and security protection of information infrastructure including servers, network environments, system status, firewalls, routers, switches and office computers, so as to prevent security risks arising from unauthorised external access and improper internal operations;

- Continuously implement anti-virus and malware protection management by deploying necessary security protection measures on servers, client devices and related terminal devices, and performing virus database updates, virus detection and removal, security testing and risk mitigation as needed;

- Prioritise the protection of data assets and back up important data and software in accordance with internal management requirements to prevent the risk of data loss, damage or irretrievability;

- Standardise the procedures for the requisition, borrowing, transmission, use, return, disposal and destruction of information storage media to reduce the leakage risk of sensitive or important information during storage, transmission and disposal;

- Adhere to the principle of least privilege, control access to information systems and permissions for data exchange to prevent unauthorised access, use, disclosure, or processing of relevant information;

- In the processes of information system development, software procurement, hardware maintenance and external services, select suppliers or service providers in accordance with procurement and contract management requirements, while clearly specifying relevant requirements regarding confidentiality, information security, service scope,

record retention and other matters in the contracts based on business needs;

- Conduct information security inspections on a regular or ad hoc basis, focusing on key areas such as hardware equipment, application systems, anti-virus software, account passwords, storage media, data backup, and employees' information security practices. The Group should address any violations of information security management requirements that cause damage to information systems, data breaches, data loss, or other adverse consequences, in accordance with relevant laws, regulations and internal policies;

- Continuously raise employees' awareness of information security. All employees are required to use work computers, email, removable storage media, third-party software and online resources in accordance with established guidelines, and avoid accessing illegal websites and using software or hardware devices from unknown sources, so as to prevent virus spread, data breaches and system damage.

This policy is overseen by the board of directors and will be reviewed and updated every three years or as and when appropriate to ensure compliance with relevant laws and regulations and to promote the continuous improvement in the Company's sustainability level.