Information Security Policy

Objective

We are committed to protecting the confidentiality, integrity, and availability of all information that supports our business operations. This includes corporate data, employee and customer information, stakeholder data, and the IT systems, networks, and applications that underpin our activities. Effective information security is essential for maintaining operational reliability, business continuity, safeguarding assets, complying with legal, regulatory, and contractual obligations, including Personal Data Protection Act 2010, and maintaining the trust of our customers, partners, and stakeholders. By managing information responsibly, we also enable sustainable business growth.

Scope

This policy applies to all information created, received, or maintained by the Company in any format, including electronic, paper-based, or verbal communication. It covers all employees, contractors, consultants, and third parties who access, process, or manage the Company's information. All personnel must protect information from unauthorized access, disclosure, modification, or loss and handle, share, and store it in accordance with the Company's procedures.

Access, Control and Handling of Information

Access to information and systems must be controlled using Role-Based Access Control (RBAC). User accounts and access rights must be created according to job roles and responsibilities, reviewed regularly and promptly revoked when no longer required. Sensitive information must be encrypted and protected at all times, and access to critical systems must be restricted to authorized personnel only.

All information must be handled securely throughout its lifecycle. This includes secure storage, transmission, and disposal. Sensitive information must be password protected where appropriate and securely destroyed when it becomes obsolete. Personnel must follow Company procedures to prevent unauthorized use, disclosure, or modification.

Data Protection and Compliance

All information, including corporate, employee, and customer data, must be handled in compliance with applicable laws and regulations, including the Personal Data Protection Act 2010 (PDPA). The Company is committed to ensuring that personal and sensitive information is collected, processed, stored, and shared in a lawful, fair, and secure manner.

Incident Management

Any actual or suspected information security incident, breach, or weakness must be reported immediately to the Administration department. Prompt reporting ensures timely investigation, mitigation, and prevention of recurrence.

Training and Awareness

All personnel must participate in periodic information security training and awareness programs to understand their roles and responsibilities in protecting Company information.

Monitoring, Review, and Governance

The Company will monitor compliance with this policy and conduct periodic reviews to address evolving risks, technologies, and regulatory requirements. The Board and Senior Management oversee information security governance, while the Administration department is responsible for implementing, monitoring, and enforcing compliance with this policy.

This Policy was adopted by the Board on 24 February 2026.