SWIRE PROPERTIES

Information Security Policy

1. Introduction

1.1 This policy (the "**Policy**") outlines the commitment of Swire Properties Limited (the "**Company**") to protecting information assets and managing information security risks across its operations.

1.2 This Policy aligns with International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)'s ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, and incorporates relevant National Institute of Standards and Technology guidance within the internal information security framework that governs its implementation.

2. Scope of application

2.1 This Policy applies to all information assets and to all employees of the Company and its subsidiaries (the "**Swire Properties Group**"), contractors, and other third parties who access or manage information on behalf of the Company.

3. Policy Statement / Principles

3.1 The Company is committed to:

- confidentiality – protecting information from unauthorised access or disclosure;
- integrity – safeguarding information from unauthorised modification; and
- availability – ensuring information and systems are accessible only when required.

3.2 These principles apply to all forms of information.

3.3 Governance

- The Company maintains an internal information security framework comprising standards, procedures, and guidelines that define control requirements, responsibilities, and implementation practices.

3.4 Risk Management and Protection

- A risk-based approach is adopted to protect information throughout its lifecycle, including appropriate controls for access, handling, retention, and disposal.
- The Company is committed to continuously improving its security posture in response to evolving risks and regulatory expectations.

3.5 Monitoring and Incident Management

- The Company maintains capabilities to monitor, detect, and respond to security threats and incidents, with defined processes for response, mitigation, recovery, and continual improvement.

3.6 Responsibilities for the Workforce

- Information security is a shared responsibility. All employees are expected to comply with applicable requirements, protect information assets, and report suspected or actual security incidents.

3.7 Third-Party Information Security Requirements

- Information security requirements are established for third parties based on risk, including appropriate due diligence and contractual obligations. All third parties are required to comply with this Policy.

3.8 Compliance

- The Company complies with all applicable information security, data protection, and privacy laws and regulations.

4. Enforcement, Compliance and Complaints

- Digital and IT Department oversees the endorsement and implementation of this Policy. This Policy is reviewed periodically to ensure continued alignment with business needs, regulatory requirements, and industry standards.