

Taziker is committed to protecting the confidentiality, integrity and availability of information entrusted to it by clients, partners, employees and other stakeholders. Information is recognised as a critical business asset that supports the delivery of construction projects, commercial operations, regulatory compliance and strategic objectives. The Company therefore establishes, implements, maintains and continually improves an Information Security Management System in accordance with ISO/IEC 27001:2023 and applicable UK legal, regulatory and contractual requirements.

The Information Security Management System applies to all information assets, whether held in electronic, physical or verbal form, and covers all business locations, construction sites, systems, processes, personnel and third parties who create, access, process or manage information on behalf of Taziker. This includes but is not limited to commercial data, design and technical information, personal data, financial records, intellectual property and operational systems supporting construction and site activities.

Taziker adopts a risk-based approach to information security, identifying and assessing information security risks and implementing appropriate controls to reduce those risks to acceptable levels. Information security controls are selected, implemented and reviewed in line with the Company's risk appetite, business objectives and the requirements of ISO/IEC 27001:2023 Annex A. Risks arising from the use of suppliers, subcontractors, joint ventures and other external parties are managed through due diligence, contractual obligations and ongoing monitoring.

Roles, responsibilities and authorities for information security are clearly defined and communicated. Senior management demonstrates leadership and commitment to the Information Security Management System by ensuring adequate resources are provided, information security objectives are established and performance is monitored. All employees and relevant external parties are required to comply with information security policies and procedures and to undertake appropriate training and awareness activities to ensure they understand their responsibilities.

Taziker is committed to complying with all applicable legal, statutory, regulatory and contractual requirements relating to information security and data protection, including the UK General Data Protection Regulation and the Data Protection Act 2018. Incidents affecting information security are reported, managed and investigated in a timely manner to minimise impact and to support continual improvement of controls and processes.

The effectiveness of the Information Security Management System is regularly reviewed through internal audits, management review and performance monitoring. The Company is committed to continual improvement of information security performance to ensure the ongoing protection of information assets, the resilience of business operations and the maintenance of trust with clients and stakeholders.

This policy is approved by top management, communicated to all relevant parties, and reviewed annually or when significant changes occur to ensure it remains appropriate to the Company's purpose, strategic direction and risk environment.



**Neil Harrison**

Managing Director

29<sup>th</sup> January 2026