1. Purpose

Taziker is committed to protecting the confidentiality, integrity and availability (CIA) of information entrusted to it by clients, partners, employees and stakeholders.

Information is recognised as a critical business asset supporting the delivery of construction projects, commercial operations, regulatory compliance and strategic objectives.

This policy establishes the framework for implementing, maintaining and continually improving an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2023 and all applicable UK legal, regulatory and contractual requirements, including UK GDPR and the Data Protection Act 2018.

2. Scope

The ISMS applies to:

- All business locations, offices and construction sites
- All systems, applications, cloud platforms and infrastructure
- All employees, directors, agency staff, subcontractors and third parties
- All information assets in electronic, physical and verbal form

3. Information Security Objectives (Clause 6.2)

Taziker establishes measurable information security objectives consistent with this policy. These objectives are reviewed at least annually during Management Review and may include:

1. Maintain zero reportable data breaches requiring ICO notification.
2. Achieve and maintain ISO/IEC 27001 certification.
3. Ensure employees complete cyber security training.
4. Maintain patching compliance above defined risk thresholds.
5. Complete scheduled internal ISMS audits and risk reviews.
6. Maintain successful backup verification and disaster recovery testing.

Objectives are measurable, monitored through defined KPIs, communicated internally, and reviewed for suitability and effectiveness. Progress against objectives is reported to Senior Management and the Board.

4. Risk-Based Approach

Taziker adopts a structured risk and opportunity management process aligned to Clauses 4.1, 4.2 and 6.1 of ISO/IEC 27001.

- Risks are identified, analysed and evaluated using a defined methodology.
- Controls are selected with reference to ISO/IEC 27001 Annex A.
- The Statement of Applicability defines applicable controls and justifies exclusions.
- Risk Treatment Plans define responsibilities and timescales.
- Residual risks are formally approved where required.
- Risks arising from suppliers, subcontractors and external partners are managed through due diligence, contractual controls and ongoing monitoring.

5. Roles and Responsibilities (RACI)

Accountable: Neil Harrison – Managing Director
Responsible: Andy Gill – IT Manager & Eddie Cairney – Data Privacy Officer
Consulted: James Keenan – Finance Director & Rob Usher – HSQE Director
Informed: All Directors, Managers and Administrative Staff

Senior Management demonstrates leadership by providing adequate ISMS resources, establishing security objectives, monitoring performance and supporting continual improvement

All employees must comply with information security policies and procedures, protect information assets, complete mandatory awareness training and report suspected incidents immediately. Failure to comply may result in disciplinary action.

6. Legal and Regulatory Compliance

Taziker complies with:

- UK GDPR
- Data Protection Act 2018
- Contractual information security requirements
- Other applicable legal and regulatory obligations

Information security incidents are reported, investigated and managed in line with IMS procedures.

7. Supporting IMS Policies & Procedures

This policy operates in conjunction with:

- Data Protection Policy
- Data Handling & Security Policy
- Personal Data Records Retention Policy
- IT Access Control Policy
- IT Data Backup Policy
- Change Management Policy
- Incident Management Procedure
- Subject Access Request Procedure
- Personal Data Breach Management Procedure

8. Monitoring, Review and Continual Improvement

The effectiveness of the ISMS is monitored through:

- Internal audits
- Risk assessment reviews
- KPI and performance monitoring
- Incident reporting and trend analysis
- Management Review meetings

The ISMS is subject to continual improvement to enhance resilience, compliance and stakeholder confidence.

The policy is reviewed at least annually or following significant organisational, regulatory or technological change.

Approved by:

Neil Harrison
Managing Director

Date: 29th January 2026