# Information Security Policy – Statement

Trowers and Hamlins (hereinafter known as the **Company**) understands the information security needs and expectations of its interested parties both within the organisation and from external parties including, amongst others, customers, clients, suppliers, partners, investors, shareholders (if applicable), regulatory and governmental departments and employees.

The Company is committed to providing the highest quality of service and we expect all members of the Company to act with professionalism. This includes maintaining information security standards and procedures. Information security is everyone's responsibility.

The Company has recognised that the disciplines of confidentiality, integrity and availability of information in Information Security Management are integral parts of its management function and view these as their primary responsibility and fundamental to best business practice.

The Company work to an Information System Management System (ISMS) which meets the requirements of International Standards ISO27001**: 2022 including the statement of applicability** which assists the company in maintaining high technical standards and a commitment to excellence in all management and administration tasks.

To this end the company has produced this Information Security Policy aligned to the requirements of ISO/IEC 27001:2022 to ensure that the Company:

The company's policies therefore are to:

- Carry out all work to high standards and to always meet or exceed the requirements of the contract and any relevant statutory regulation.
- Implements Information Security Objectives that consider information security requirements following the results of applicable risk assessments.
- Communicates these Objectives and performance against them to all interested parties.
- Works closely with customers, business partners and suppliers in seeking to establish appropriate information security standards.
- Adopts an Information Security Management System comprising a Security Manual and Procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers, and other interested parties who come into contact with its work.
- Adopts a forward-thinking approach on future business decisions, including the continual review of risk evaluation criteria, which may impact on information security.
- Identify and comply with all applicable statutory/legal requirements that relate to environmental aspects with a view to being carbon neutral and the prevention of pollution in relation to any of the Company's work activities.
- Enhance the Company's Security performance.
- Works closely with employees, customers, business partners and suppliers in seeking to establish appropriate information security standards;
- Instructs all members of staff in the needs and responsibilities of Information Security Management;
- Constantly strives to meet, and where possible exceed, its customer's expectations;
- Implements continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to better meet information security requirements.
- Commit to provide safe and healthy working conditions for the prevention of work-related injury/or ill health that is appropriate to the purpose, the size and context of the Company.

Responsibility for the company's ISMS policy lies with the Director of Information Services.

This policy is publicly available on request.

Signed on behalf of the Management:

Richard Elson
Director of Information Services

Issue Date: 06 Jan 2023

Review Date: 10 April 2026