Information security policy statement

This statement applies to all business activities, all Troup Bywaters + Anders LLP (TB+A) employees and associated sub-consultants and suppliers in relation to their contractual requirements, who share a responsibility for the security of services provided to clients and the protection of associated information. This policy statement will also be made available to interested parties on our website and upon request.

We recognise that the information is a key business asset of significant value and needs to be suitably protected. As a custodian of both client and employee information, we are committed to protect and manage this information from unauthorised modification, loss, or accidental or deliberate disclosure to meet the requirements of the UK GDPR and Data Protection Act 2018, and to enable TB+A to meet its contractual, legislative, privacy and ethical responsibilities.

To meet this commitment, we have implemented an Information Security Management System (ISMS) to meet the relevant requirements of ISO 27001:2022 comprising policies, plans, processes and controls covering physical, personal, IT and documentation assets. The effective implementation of the ISMS policies and procedures will assist in the achievement of our key objectives, enhance reputation and protect confidentiality, integrity and availability of both company and client information.

The Board are responsible for the effective implementation of the ISMS, as well as the establishment of detailed information security objectives and the monitoring of their achievement on a regular basis. The ISMS Management Team are responsible for the management, monitoring, auditing, effectiveness reporting of the day-to-day implementation.

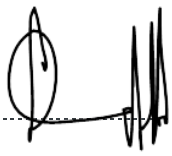
We are committed to satisfying client expectations and that the services offered meet contractual requirements.

All employees are made aware of this policy and its importance through our company intranet, supported by training and ongoing refreshers and awareness. Business Unit Leaders are responsible for implementing the policy within their business areas. Visitors will be made aware of and comply with this policy along with applicable ISMS requirements.

It is the policy of our Partnership to see that:

+ Roles are responsibilities are defined for the execution of information security activities. These can be found within our Integrated Management System (IMS) procedures
+ AI usage is supported by policies and procedures to maintain user privacy and comply with data protection and other relevant legal requirements. See separate AI Policy for further details
+ Regularity and legislative requirements regarding data protection and privacy of personal information are met
+ Business continuity plans will be produced, maintained, and tested
+ Employees receive sufficient Information Security briefing on projects that are classed as confidential or sensitive
+ Breaches of Information Security that result in a risk to people's rights and freedoms under the UKGDPR, i.e. discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage, will be investigated and reported without undue delay and where feasible, within 72 hours
+ Risk assessments are undertaken routinely and risks are placed under applicable ISMS controls for their ongoing protection
+ We continually improve the Information Security Management System

Action will be taken in the event of a violation of this policy.

Signed:  James Campbell – Managing Partner

Date: 2nd March 2026

Next review date Jan 2027