TROUP BYWATERS + ANDERS

Security policy statement

Troup Bywaters + Anders LLP recognises that information is an important business asset of significant value to the company and needs to be protected.

The purpose of this Policy is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental.

This Policy also applies to personal data and its protection from unauthorised access, dissemination and loss.

The policy covers Physical Security and encompasses all forms of Information Security such as data stored on computers, servers or cloud based hosts, transmitted across networks or email, printed or written on paper, stored on any type of storage disk/device or spoken in conversation or over the telephone.

Specific metrics used to track the success of this policy are included in our Context of the Organisation document and are discussed at Management review twice a year.

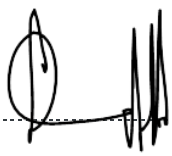
All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their employees.

It is the responsibility of each employee to adhere to the policy.

It is the policy of our Partnership to see that:

+ Information will be protected against unauthorised access
+ Roles are responsibilities are defined for the execution of information security activities. These can be found within our Integrated Management System (IMS) procedures
+ A "proceed with caution" approach to AI usage is strongly encouraged to maintain user privacy and comply with data protection and other relevant legal requirements. See separate AI Policy for further details
+ Confidentiality and security of information is assured
+ Integrity of information is maintained
+ Regularity and legislative requirements regarding data protection and privacy of personal information are met
+ Business continuity plans will be produced, maintained, and tested
+ Staff receive sufficient Information Security briefing on projects classed as confidential
+ Breaches of Information Security that result in a risk to people's rights and freedoms under the GDPR, 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
+ Training will be undertaken by our employees on information security awareness, including refresher training
+ 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 January 2026

Next review date Jan 2027