CLEAR QUALITY

Information Security Policy

Purpose

This information security policy specifies management's intent to protect all important information assets within Clear Quality from all threats, whether internal or external, deliberate, or accidental. Information within Clear Quality exists in many forms and this policy applies to and includes the protection of data stored electronically, transmitted across networks, and printed or written on paper. The prime purpose of this Information Security Policy is to protect and safeguard the information of the firm's clients and customers. The needs and expectations of all interested parties have been considered in the development of this security policy.

Objectives

The objective of information security is to ensure business continuity and minimise damage by preventing and reducing the impact of security incidents. The implementation of this policy is mandatory to maintain and demonstrate the firm's integrity in dealings with all our customers, clients, and trading partners.

It is the policy of Clear Quality to ensure:

- Information is protected against unauthorised access.
- Confidentiality of information is assured.
- Information is not disclosed to unauthorised persons through deliberate or careless actions.
- The integrity of information is maintained.
- The availability of information to authorised users when needed.
- Regulatory and legislative requirements are met.
- Business continuity plans will be produced, maintained, and regularly tested.
- Information security training will be given to all staff.
- All breaches of information security, actual and suspected are recorded reported and investigated.
- That it is compliant with best practice as identified in ISO/IEC 27002 and meets all the criteria specified within BS ISO/IEC 27001 2022. The company will seek formal certification to this standard.
- All staff have been provided with user training and awareness in respect of their work, information assets and the policies and procedures associated with achieving the above objectives. Records of this training have been maintained.

Standards, policies and security operating procedures will be produced to support this policy and will include virus control, access control, personnel security, the use of e-mail and the Internet. A formal disciplinary process is documented and implemented when necessary to address issues arising with employees who choose not to comply with these standards, policies, and procedures.

The effectiveness of controls will be measured wherever it is practicable to do so, the results analysed, and improvements will be implemented where identified, as necessary.

Where it is impractical to measure controls, they will be monitored for effectiveness. When identified continual improvement of the ISMS will be actioned/implemented as appropriate.

The Managing Director has overall responsibility for maintaining this Policy and providing guidance on its implementation. All consultants are personally responsible for implementing the policies and procedures within their business areas. It is the responsibility of each employee to adhere to the policies and procedures in their areas.

This policy will be reviewed regularly to ensure it remains appropriate for the business and the company's ability to achieve the company's security objectives and serve its customers.