QEISR02C Information Security Policy

(ISO/IEC27001: 2022 Clause 5.2)

The Senior Leadership Team at Clear Connections Holdings Limited understands the information security needs and expectations of its interested parties, both within the organisation and from external parties, including, amongst others, clients, suppliers, regulatory and Governmental departments. 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 views these as its primary responsibility and fundamental to best business practice. To this end, Clear Connections Holdings Limited has produced this Information Security Policy aligned to the requirements of ISO/IEC 27001:2022 to ensure that the Company:

- Complies with all applicable laws, regulations, and contractual obligations.
- 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.
- 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.
- Works closely with customers, business partners and suppliers in seeking to establish appropriate information security standards.
- Adopts a forward-thinking approach to future business decisions, including the continual review of risk evaluation criteria, which may impact information security.
- Instructs all members of staff in the needs and responsibilities of Information Security Management.
- Constantly strives to meet, and where possible exceed, its customers' expectations.
- Implements continual improvement initiatives, including risk assessment and risk treatment strategies, while making the best use of its management resources to meet information security requirements better.

Responsibility for upholding this policy is company-wide under the authority of the Managing Director, who encourages all staff to make a personal commitment to addressing information security as part of their skills.

This policy is available to and communicated to all interested parties, as well as made available to the broader community through publication on our website, company noticeboard, and intranet.

Authorised by:	Steve Walker	Position:	Managing Director
Date Approved:	31/05/2025	Review Date:	May 2026