

## Information Security Policy

Effective: 2026

Quicksilver is committed to safeguarding the confidentiality, integrity, and availability of all physical and electronic information assets of the organisation. This commitment ensures that regulatory, operational, and contractual requirements are fulfilled.

## Information Security Objectives:

The overall goals for information security at Quicksilver are to:

- Ensure compliance with all applicable laws, regulations, and guidelines.
- Protect the confidentiality, integrity, and availability of information for Quicksilver employees, contractors, clients, and other authorised users.
- Establish and maintain appropriate controls to protect Quicksilver information and information systems against theft, misuse, unauthorised access, damage, and loss.
- Promote a culture of responsibility, ownership, and awareness of information security among management and staff to minimise the risk of security incidents.
- Ensure Quicksilver can continue critical services and operations in the event of major information security incidents or disruptions.
- Ensure the protection of personal data and respect for individual privacy in accordance with applicable data protection laws.
- Maintain the availability, reliability, and resilience of network infrastructure and information systems operated or used by Quicksilver.
- Align information security practices with recognised international standards, including ISO/IEC 27001 and related frameworks.
- Ensure that external service providers and third parties handling Quicksilver information comply with Quicksilver's information security requirements.

## Scope

*This policy applies to all Quicksilver employees, contractors, temporary staff, and third parties who access, process, store, or manage Quicksilver information or information systems.*

