# ISMS Policy Statement

As a modern, forward-looking business, Kirby Group recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders, and other stakeholders.

Kirby Group is committed to establishing clear and effective Information Security policies to protect its key business activities and meet its obligations to interested parties, including customers, shareholders, employees, and suppliers.

As part of this commitment, Kirby Group has established an Information Security Management System (ISMS) that complies with the requirements of the ISO 27001 international standard for information security and will be seeking to maintain the compliances to this standard.

It is the policy of Kirby Group to:

- Make the Information Security Policies available and communicated within the organisation and to all relevant stakeholders and interested third parties.
- Define various roles within the ISMS together with their relevant responsibilities and levels of authority
- Ensure all employees are trained, competent and made aware of their individual obligations
- Adopt an Information Security Management System ("ISMS") comprising an overarching policy document/manual, policies and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers, and other interested parties
- Define clear objectives, and a system of monitoring and measurement established to record progress against targets, in alignment with a continual risk assessment.
- Regularly set, review and update objectives for information security as an essential part of the continual improvement of the ISMS
- Safeguard security of the information assets through effective business continuity management and disaster recovery based on Business Impact Analysis.
- Provide with specific resources required in addition to:
    - Human Resources
    - Technical Resources
    - Information Resources
    - Financial Resources
- Protect the information collected and used for the benefit of the organisation and its customers from all threats whether internal or external, deliberate, or accidental
- Comply with all applicable laws, legal, regulations and contractual obligations
- Report all actual or suspected information security incidents and breaches
- Ensure the Integrity, Confidentiality and Availability of information are maintained

The policy has been approved by Digital Construction and IT Director and is reviewed annually or sooner should a significant change occur to ensure its continuing suitability, adequacy, and effectiveness.
The Information Security Management System is subject to both internal and external annual audits.

Date: 06/01/2025

Signed: 

Version 1
Issued on: 06 January 2025

Mark Danaher
Digital Construciton and IT Director