Specialist Joinery Manufacturers

James Johnson & Co Ltd

INFORMATION SECURITY POLICY STATEMENT

Objective:

The purpose and objective of James Johnson & Co Ltd ‘s Information Security Policy is to protect the company’s information assets (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise damage to the business and maximise return in investment and business opportunities.

Policy:

It is the Policy of James Johnson & Co to ensure that:

a) Information will be protected from a loss of confidentiality (note 2), integrity (note 3) and availability (note 4).
b) Regulatory and legislative requirements will be met (note 5).
c) The Business Continuity Plan will contain actions relating to information security.
d) Information Security training will be available to relevant staff.
e) All breaches of information security, actual or suspected, must be reported to a Managing Director and consequently investigated.

Guidance and procedures will be produced as required within the company’s integrated management system to support this policy.

The company has engaged the services of competent agents to handle its information technology requirements, including management of issues relating to information security.

The Joint Managing Director whose signature appears on this policy is the owner of the Policy and will review the policy annually.

All managers are directly responsible for implementing this policy within their business areas.

It is the responsibility of each worker to adhere to the Information Security Policy

Signed:  **Paul Ridley**

Date: February 2023

Position: Joint Managing Director

NOTES:

1. Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation.
2. Confidentiality: ensuring that information is accessible only to authorised persons.
3. Integrity: safeguarding the accuracy and completeness of information and processing methods.
4. Availability: ensuring that authorised users have access to information when required.
5. This includes the requirements of The Data Protection Act (1998), The Data Protection (Processing of Sensitive Personal Data) Order 2000, The Copyright, Designs and Patents Act (1988), The Computer Misuse Act (1990), The General Data Protection Requirements Regulations 2018