

Information Security

Policy

The objective of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

The purpose of this policy is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of the organisation to ensure that:

Information will be protected against unauthorised access

Confidentiality of information will be maintained

Integrity of information will be maintained

Availability of information is ensured as required by the business process

Regulatory and legislative requirements will be met

Business continuity plans will be produced, maintained and tested

Information security training will be available to all staff

All breaches of information security, actual or suspected will be reported to, and investigated by the information security manager

The organisation operates processes and procedures to support this policy.

It is the responsibility of each member of staff to adhere to the policy.

The Information Security Policy of the organisation has been prepared after due consultation with those involved in its operation and has the full backing and authority of the Directors.

Approved by:

Dave Pattinson

Managing Director

Issue Date:

4th March 2022

Last Review Date:

9th August 2024

Next Review Date

9th August 2025

Ref: PV 04

This policy will be reviewed annually or earlier if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.