Information Security Policy

Policy Statement

SGC Holdings Ltd recognises the importance of protecting the information it holds and uses in the course of its business. This policy sets out the Company's approach to managing information security and reducing the risk of unauthorised access, loss, misuse, or disruption.

The Company is committed to maintaining appropriate technical and organisational measures to protect information and information systems and to meeting its legal, regulatory, and contractual obligations, including those relating to Cyber Essentials.

Scope

This policy applies to all information processed by SGC Holdings Ltd, whether held electronically or in paper form, and to all systems, devices, and networks used to store or process that information.

It applies to all employees, contractors, agency staff, and third parties who have access to Company information or systems.

Responsibilities

Senior management has overall responsibility for ensuring that appropriate information security arrangements are in place.

Managers are responsible for ensuring that employees within their areas understand and comply with this policy.

All users are responsible for:

- Protecting information they access or handle
- Using Company systems in accordance with this policy
- Reporting any actual or suspected security incidents without delay

Information Classification

Information must be handled in a manner appropriate to its sensitivity.

Information is classified as:

- Public

- Internal
- Confidential
- Restricted

The level of protection applied must reflect the classification of the information.

Access Control

Access to systems and information is granted on the basis of business need.

- User accounts must be unique
- Access rights must be approved and reviewed
- Access must be removed promptly when no longer required
- Privileged access must be restricted and monitored

Passwords and Authentication

Users must keep passwords secure and confidential.

- Passwords must meet minimum complexity requirements
- Password sharing is not permitted
- Default passwords must be changed before systems are used
- Multi-factor authentication must be used where supported

Secure Systems and Configuration

Company systems must be configured securely and maintained to reduce vulnerabilities.

- Unsupported or end-of-life systems must not be used
- Security updates and patches must be applied promptly
- Only authorised software may be installed

Malware Protection

Appropriate malware protection must be in place on all Company devices.

- Protection must be kept up to date
- Users must not disable or bypass security controls

Data Storage, Retention and Disposal

Information must be stored securely and retained only for as long as necessary.

When information or equipment is no longer required, it must be disposed of securely in accordance with Company procedures.

Incident Management

All information security incidents, including suspected data breaches, must be reported immediately.

Incidents will be investigated and managed in accordance with Company procedures and, where required, escalated to senior management or relevant authorities.

Third Parties

Where third parties are given access to Company systems or information, appropriate security controls and contractual safeguards must be in place.

Compliance and Review

Failure to comply with this policy may result in disciplinary action.

This policy will be reviewed regularly and updated where necessary to reflect changes in technology, business operations, or legal requirements.

Name	Paul Macarthur	Position	Managing Director
Signature		Date	14/01/2026