Purpose: This policy outlines Steve J Martin Ltd's commitment to protecting our information assets from cyber threats. It establishes the framework for cybersecurity management within our organization.

Scope: This policy applies to all employees, contractors, and visitors to our workplace, as well as our information systems, networks, and data.

Policy Statement: Steve J Martin Ltd is committed to:

- Protecting our information assets from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Complying with all applicable cybersecurity laws and regulations.
- Continuously improving our cybersecurity practices.

Responsibilities:

- **Management:**
  - Develop and implement cybersecurity policies and procedures.
  - Ensure adequate resources are allocated for cybersecurity.
  - Monitor and review cybersecurity performance.
  - Investigate cybersecurity incidents to identify root causes and prevent recurrence.
- **IT Department:**
  - Develop and implement technical security measures.
  - Monitor cybersecurity risks and threats.
  - Respond to cybersecurity incidents.
  - Provide cybersecurity training and awareness.
- **Employees:**
  - Comply with cybersecurity policies and procedures.
  - Report any cybersecurity incidents or suspicious activity.
  - Participate in cybersecurity training.

Risk Assessment:

- Regular risk assessments will be conducted to identify potential cybersecurity threats and vulnerabilities.
- Appropriate controls will be implemented to mitigate risks.

Access Controls:

- Access to information systems and data will be restricted to authorized users.
- Access controls will be implemented to prevent unauthorized access.
- Regular reviews of access rights will be conducted

Password Management:

- Employees will be required to use strong, unique passwords for their accounts.
- Password policies will be enforced to prevent the use of weak or easily guessable passwords.

Data Protection:

- Sensitive data will be protected using appropriate security measures.
- Data will be encrypted both at rest and in transit.
- Regular backups will be performed to ensure data recovery in case of a breach.

Incident Response:

- An incident response plan will be developed and regularly tested.
- Cybersecurity incidents will be reported and investigated promptly.
- Appropriate measures will be taken to contain and mitigate the impact of incidents.

Employee Awareness:

- Employees will receive training on cybersecurity best practices.
- Awareness campaigns will be conducted to promote cybersecurity awareness.

Supplier Security:

- We will require our suppliers to adhere to cybersecurity standards.
- Supplier security will be assessed as part of our procurement process.

Review and Improvement:

- This policy will be reviewed annually to ensure its effectiveness.
- Continuous improvement measures will be implemented to enhance our cybersecurity posture.

Steve Martin
Company Director

Steve Martin