Information Security Policy

1. Purpose
This policy establishes minimum Information Security requirements for SMEs in New Zealand and Australia. It outlines the organisation's commitment to safeguarding data, systems, and digital services.

2. Scope
This policy applies to all employees, contractors, consultants, partners, and third parties who access organisational information systems.

3. Governance & Accountability
• Maintain an Information Security Management Framework.
• A designated Security Lead or vCISO is accountable for information security.
• All staff must comply with the NZ Privacy Act 2020, Australian Privacy Act 1988 (APPs), and applicable regulations.

4. Risk Management
• Conduct annual risk assessments and maintain a risk register.
• Implement risk treatments aligned to ISO 27001, NIST CSF, Essential Eight.
• Review risks quarterly or during significant organisational changes.

5. Access Management
• Enforce least privilege and role-based access.
• MFA required for all cloud and remote systems.
• Privileged accounts must be tightly controlled and periodically reviewed.

6. Data Protection & Privacy
• Classify and protect information based on sensitivity.
• Apply encryption for data in transit and at rest.
• Ensure compliance with NZ Privacy Act, APPs, PDP Act (Victoria) and GDPR (if applicable).

7. Acceptable Use
• Users must follow acceptable use guidelines for devices, networks, and digital tools.
• Prohibited activities include unauthorised access, harmful downloads, and misuse of data.

8. Incident Management
• Incidents must be reported promptly.
• Maintain an incident response plan and run annual exercises.
• Escalate to Secompass or equivalent partners when needed.

9. Business Continuity & Backups
• Maintain regular backups and test restoration twice annually.
• Ensure BCP covers cyber risks and operational disruption scenarios.

10. Vendor & Third-Party Security
• Assess vendors handling sensitive data.

• Maintain contracts requiring compliance with security and privacy standards.

11. Training & Awareness
• Conduct annual cyber awareness training.
• Provide targeted training for privileged users and IT teams.

12. Policy Review
This policy must be reviewed annually or following significant regulatory or organisational changes.