1. Purpose

The purpose of this Information Security Policy is to protect **Setec Consulting Engineers Ltd (SCEL)'s** information assets from all internal, external, deliberate, or accidental threats, ensuring business continuity, minimising business damage, and maximising return on investments and business opportunities in accordance with ISO 27001 and applicable U.K. regulations.

2. Scope

This policy applies to all SCEL employees, contractors, consultants, temporary staff, and third-party service providers who access SCEL's information systems and data.

3. Information Security Objectives

- Maintain the confidentiality, integrity, and availability of information assets.
- Comply with ISO 27001, the UK GDPR, and other applicable legal and regulatory requirements.
- Manage risks to information security effectively.
- Ensure that information security is an integral part of all business processes.

4. Governance and Responsibilities

- **Managing Director:** Ultimate responsibility for information security.
- **Information Security Manager (ISM):** Oversees the implementation of this policy and ISO 27001 controls.
- **Data Protection Officer (DPO):** Manages compliance with UK GDPR and data protection policies.
- **All Employees:** Responsible for adhering to this policy and reporting security incidents.

5. Risk Management

- Regular risk assessments shall be conducted to identify, assess, and mitigate information security risks.
- Implementation of appropriate controls to manage identified risks.

6. Access Control

- Access to information and systems is granted on a need-to-know and least privilege basis.
- All users must authenticate using secure methods (e.g., strong passwords, multi-factor authentication).

7. Data Protection

- Processing of personal data shall comply with the UK GDPR.
- Personal data must be collected for specified, explicit, and legitimate purposes.
- Personal data must be protected against unauthorised access, processing, and loss.

8. Physical and Environmental Security

- Physical access to SCEL offices and data centers shall be restricted to authorized personnel.
- Environmental controls must be in place to protect against fire, flood, and other hazards.

9. Incident Management

- All information security incidents must be reported to the ISM immediately.
- Incidents will be logged, investigated, and remediated in a timely manner.

10. Business Continuity

- Business continuity and disaster recovery plans shall be established, maintained, and regularly tested.
- Critical information and systems must be backed up regularly and securely stored.

11. Compliance

- SCEL shall comply with all applicable legal, regulatory, and contractual information security requirements.
- Regular audits shall be conducted to ensure compliance with ISO 27001 and internal policies.

12. Training and Awareness

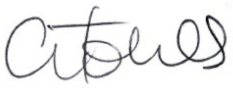
- Regular information security training shall be provided to all employees.
- Specialised training will be provided to personnel with specific security responsibilities.

13. Policy Review

- This policy shall be reviewed annually or upon significant changes in business operations or legal requirements.
- The ISM is responsible for coordinating the review and update of this policy.

This policy is designed to complement the SCEL's Data Protection Policy (SCEL-POL-01-109) and aligns with our commitment to protecting information and ensuring compliance with ISO 27001 and relevant U.K. regulations.

Signed:



Grant Jones
Managing Director, SCEL
Date: 13/05/2025
Next Review Date: 13/05/2026

Employee Declaration

Read & Signed by:	
Name:	
Signature:	
Date:	

By signing this document you are confirming that you have read, understood and agreed with your responsibilities.