INFORMATION SECURITY POLICY

1. POLICY STATEMENT

As Secto, we are committed to securing and protecting our information assets and those of our clients, ensuring confidentiality, integrity, and availability in line with ISO 27001:2022 requirements. We recognise the importance of information security in maintaining trust, delivering excellence, and supporting our strategic objectives. Our policy mandates compliance with applicable legal, regulatory, and contractual obligations. We continuously improve our Information Security Management System (ISMS) through regular review, risk assessment, and mitigation strategies, engaging our entire workforce in upholding our information security standards.

2. SCOPE

This policy applies to all employees, contractors, and third-party vendors of Secto Services Ltd, encompassing all operational areas, including but not limited to commissioning, operational maintenance, and engineering support services.

3. PRIMARY OBJECTIVES

- **Confidentiality:** Only authorised individuals have access to information.
- **Integrity:** Information is accurate, complete, and protected against unauthorised modification.
- **Availability:** Information and critical services are available to authorised users when needed.

4. POLICY PRINCIPLES

- **Risk Management:** Conduct periodic risk assessments to manage and mitigate information security risks.
- **Employee Responsibility:** Employees are obliged to adhere to this policy and related security procedures.
- **Incident Management:** Establish a robust incident management process for the swift identification and resolution of security breaches.
- **Continuous Improvement:** Continuously review and enhance the ISMS to address emerging threats and business needs.

5. ROLES AND RESPONSIBILITIES

- **Management:** Align the Information Security Policy with strategic business objectives.
- **ISMS Team:** Implement, oversee, and improve the ISMS.
- **Employees:** Comply with the Information Security Policy and procedures.

6. POLICY ENFORCEMENT

Failure to comply with this Information Security Policy may result in disciplinary action, up to and including termination of employment or contracts. Violations will be dealt with promptly and in accordance with Secto's disciplinary procedures.

7. REVIEW AND REVISION

This policy will be reviewed annually or following significant changes to the business, technology, or legislation to ensure its continuing suitability, adequacy, and effectiveness.

Signed: 

Title: COO

Name: Aidan Barry

Date:03/04/2024