Roscan Electronics Ltd.

Information Security Policy

Code:	WI.18
Version:	1.0
Created by:	C. Withers
Date of version:	10.10.24

Distribution list

Copy No.	Distributed to	Date	Returned	
			Date	Signature

Change history

Date	Version	Created by	Description of change
10.10.24	1.0	C. Withers	Basic document outline

1. Purpose, scope and users

Roscan Electronics Ltd. is committed to maintaining the highest standards of information security to protect sensitive customer data, samples, drawings, and any other information supplied by customers. This policy outlines the measures and procedures in place to ensure the confidentiality, integrity, and availability of such information. This policy applies to all employees, contractors, and third-party partners of Roscan Electronics Ltd. who handle sensitive customer information.

2. Objectives

- To document how sensitive information is controlled.
- To ensure compliance with ISO 9001:2015 standards.
- To protect customer data from unauthorised access, disclosure, alteration, and destruction.

3. Reference document

- PR.03 Quality Manual
- WI.17 Third-Party Data Breach Procedure

4. Roles and Responsibilities

4.1. QA & Projects Director

- Oversee the implementation and maintenance of this policy.
- Conduct regular security audits and risk assessments.
- Ensure compliance with relevant standards and regulations.

4.2. Employees

- Adhere to the information security policies and procedures.
- Report any security incidents or breaches immediately.

4.3. IT Department

- Implement technical controls to protect sensitive information.
- Monitor and respond to security threats.

5. Information Security Controls

5.1. Identification

- When specified by the owner, sensitive information will be clearly identified as such.

5.2. Access Control

- Access to sensitive information is restricted to authorised personnel only.
- The use of removable media must be authorised by senior management.
- Multi-factor authentication is required for accessing sensitive systems.
- IT department restricts and authorises the installation of applications

5.3. Data Handling

- Sensitive information will be encrypted during transmission and storage when requested by the owner.
- Physical copies of sensitive information must be stored in secure, locked locations when requested by the owner.

5.4. Data Retention and Disposal

- Sensitive information is retained only as long as necessary for business purposes.
- Secure disposal methods are used for both physical and digital information.

6. Incident Management

6.1. Reporting

- All security incidents must be reported to the QA & Projects Director immediately.
- Use the WI.17 Third-Party Data Breach Procedure for incidents involving third parties.

6.2. Response

- The Information QA & Projects Director will coordinate the response to security incidents.

- Affected parties will be notified as required.

7. Training and Awareness

- Awareness campaigns to highlight the importance of information security.

8. Compliance and Review

- Regular audits to ensure compliance with this policy and ISO 9001:2015 standards.
- This policy will be reviewed annually and updated as necessary.