INFORMATION SECURITY POLICY

This applies to the Director and associated persons of EDGEidesign Ltd.

1 Policy Statement

1.1 The purpose of this Policy is to protect the confidentiality, integrity, and availability of the organisation's information assets. This policy establishes mandatory security requirements for all employees, consultants, and third-party suppliers.

2 Responsibilities

2.1 The Director is responsible for:

- overall information risk governance and ensuring compliance
- implementing controls, monitoring compliance, and managing incidents
- the security of specific information assets (e.g. project data)

3 Information Security Objectives

3.1 The organisation will:

- protect information from unauthorised access or disclosure
- ensure accuracy, completeness, and reliability of information
- maintain availability of systems and data to support business operations
- comply with legal, regulatory, and contractual obligations
- embed Security by Design into all project and operational processes
- continually improve the information security management

3.2 Where relevant the organisation will comply with:

- UK GDPR and Data Protection Act 2018
- NIS Regulations 2018
- Copyright, Designs and Patents Act 1988
- Contractual confidentiality obligations
- CIAT professional standards

4 Information Classification & Handling

4.1 Classification Levels:

- Public – Approved for public release
- Internal – For internal use only
- Confidential – Sensitive business or client information
- Restricted – Highly sensitive information requiring enhanced controls

4.2 Handling Requirements

- Use encryptions for all Confidential and Restricted data
- Store project data on secured server only
- Do not email sensitive data without encryption
- Follow secure disposal procedures for all media

5 Physical & Environmental Security

- Confidential waste must be shredded or securely disposed
- ICT equipment is secure and password protected or physically locked

6 Technical Security Controls

- All ICT equipment is protected by antivirus software
- Operating systems and applications must be patched within 7 days of release
- Firewalls must be configured and monitored
- Backups must be encrypted, tested, and stored securely
- Cloud services must meet security requirements (e.g. QNAP cloud services certified to ISO 27001)

7 Secure Development & Project Delivery

- Ensuring secure sharing of reports, commercial data. specifications, models and drawings
- Using known common data environment platforms
- Applying access controls to project folders

8 Incident Management

- The Director will assess the severity, contain the incident, and coordinate a response
- Personal data breaches must be reported to the ICO within 72 hours if required

9 Business Continuity & Disaster Recovery

- The office data server is locked secure and backed up in a remote location
- Backups must be tested regularly

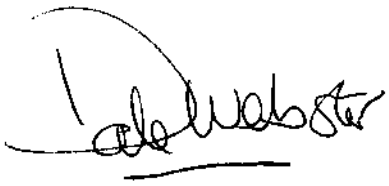
10 Monitoring, Audit & Continuous Improvement

- Systems and logs will be monitored for suspicious activity
- System security notifications and audits will assess compliance
- Non-conformities will be recorded and addressed
- This policy will be reviewed annually or after major incidents

Please contact the Director, Dale Webster, if you wish to discuss any issue that is covered by this policy. EDGEidesign Ltd reserves the right to change this policy prior to the review date where exceptional circumstances apply.

The Director of EDGEidesign Ltd approved this policy on the 10th September 2025.

Signed:



Dale Webster, Director
(Signed on behalf of EDGEidesign Ltd)

Next review date: September 2026