Level 5 Lifestyle Distributors Ltd

Security Overview

Our approach to information security and data protection

1. Introduction

We take security seriously. Public sector clients trust us with their systems and data, and we treat that as a practical responsibility rather than something to tick off a list.

This document sets out our security controls and practices. It is intended to support procurement evaluations and give clients a clear picture of how we work.

2. Cyber Essentials Certification

Cyber Essentials is a UK Government-backed certification scheme covering five core security control areas. We are currently working through the certification process.

Cyber Essentials (March 2026)	**IN PROGRESS**

The five control areas covered are:

- Firewalls: boundary devices configured to block unauthorised access
- Secure configuration: systems set up with unnecessary features removed
- User access control: least-privilege access, strong authentication, and regular access reviews
- Malware protection: endpoint protection against malicious code
- Patch management: security updates applied promptly across all software and systems

3. Data Protection & GDPR Compliance

We build data protection in from the start rather than adding it later. Our approach follows the UK GDPR and the Data Protection Act 2018.

Privacy by Design	Privacy and data minimisation are considered at the architecture stage, not retrofitted after the fact.
Data Minimisation	We collect only what is needed for each service. Unnecessary data is not kept.
Documented Data Flows	Data flows are documented as part of project delivery, which helps clients with their own DPIA requirements.
Retention & Deletion	Retention periods are agreed with clients up front. Deletion procedures are documented and followed.
Lawful Basis	We map processing activities to the appropriate lawful basis before building anything.

4. Infrastructure & Hosting Security

We use UK-based or UK-GDPR-compliant cloud hosting providers for all client systems. Hosting environments are set up as follows:

- HTTPS enforced on all public-facing services, TLS 1.2 minimum
- Infrastructure access restricted to named personnel via SSH key authentication
- No default passwords. All credentials are unique, rotated regularly, and stored in a password manager
- Staging and production environments kept fully separate
- Automated backups with restore procedures tested periodically
- Database access restricted to the application layer only

5. Secure Development Practices

Security is part of how we build things, not a box to tick before going live:

- OWASP Top 10 used as a baseline for web application security assessment
- Dependencies reviewed for known vulnerabilities using automated scanning tools
- Code reviews required before merging changes to production branches
- Version control via Git with protected main branches and audit trails
- Input validation and output encoding applied to all user-facing interfaces
- Authentication uses established libraries. We do not write custom auth logic
- Security testing carried out as part of pre-launch review for all projects

6. Incident Response

If a security incident affects a client system or data, we will:

- Notify the affected client within 24 hours of becoming aware of a potential breach
- Provide an initial assessment of the scope and impact within 48 hours
- Work with the client to contain and remediate the incident as a priority
- Support the client in meeting their ICO reporting obligations where required (72-hour notification window)
- Conduct a post-incident review and provide a written report on findings and remediation steps

7. Access Controls & Personnel

Access to client systems and data is controlled on a strict least-privilege basis:

- Access granted only to personnel who require it for the specific project
- All access is logged and reviewed at project milestones
- Access is revoked promptly upon project completion or staff change
- All staff handling client data are briefed on data protection obligations
- Sub-contractors and freelancers are required to comply with our security standards and sign appropriate agreements before accessing any client system or data

8. Supply Chain Security

When working with sub-contractors or technology partners, we carry out the following checks:

- Third-party tools and platforms assessed for security and GDPR compliance before use
- Open source dependencies reviewed for known vulnerabilities prior to inclusion
- Sub-contractors bound by confidentiality and data protection obligations via written agreements
- Technology stack uses open standards to avoid vendor lock-in and ensure replaceability

9. Security Contact

For security queries, vulnerability disclosures, or any questions about how we work, get in touch:

Haf Saba — Founder & Security Lead
Email: enjoy@level5.life
Web: www.level5.life/gov

This document is correct as at March 2026 and will be updated following Cyber Essentials certification.