SKYLARK SPHERE LTD

Information Security Policy

SKYLARK SPHERE LTD | Version 1.0 | Effective 22 September 2026 | Next review September 2027 | Owner: Director

Summary. This policy sets out the information security programme of SKYLARK SPHERE LTD: who is responsible, the controls we apply to our network, servers, endpoints and daily operations, and the supporting policies that make up the programme.

Purpose and scope

We build and operate software, SaaS products and e-commerce systems. Many of these process data belonging to our clients and their customers, including data received from online marketplaces and sales channels through their APIs. This policy exists so that information is only accessed by the right people, stays accurate, and is available when needed.

It applies to all directors, employees, contractors and anyone else with access to our systems ("personnel"), and to every system, device, account and environment we use to store or process company, client or personal data.

Roles and responsibilities

- **Director (Security Owner):** accountable for the security programme, approves policies, owns risk decisions and leads incident response.
- **Personnel:** follow this policy and the supporting policies, complete security onboarding, and report suspected incidents immediately.
- **Contractors and suppliers:** may only access data they need for their work, under written confidentiality terms.

Security programme

Our programme consists of this policy and the following supporting documents, all published in our trust centre:

- Access Control Policy
- Data Classification and Encryption Policy
- Incident Response Policy

- Vulnerability and Threat Management Procedure
- Data Protection Policy and our public Privacy Policy

We assess information security risks at least annually and whenever we introduce a new system, supplier or type of data, and record the actions we take.

Network security and segregation

- Production systems run on dedicated hosted servers, separate from personnel devices and from development environments. Development and testing never use live personal data unless it is essential and approved.
- Server firewalls deny inbound traffic by default and allow only the ports required for the services we provide.
- Databases and internal services listen only on private interfaces and are never exposed directly to the internet.
- Administrative access (SSH and control panels) requires strong authentication, and repeated failed logins are blocked automatically by intrusion prevention (fail2ban).
- All web traffic is served over HTTPS with HSTS and modern TLS. Security headers are set on our websites.
- Server and application logs are kept and reviewed to detect suspicious activity, failed logins and unusual traffic.

Endpoint protection (anti-virus)

- Every company laptop and workstation runs anti-malware protection with real-time scanning and automatic signature updates (Microsoft Defender on Windows, XProtect on macOS, or an approved equivalent).
- Servers run ClamAV anti-malware scanning.
- Operating systems and browsers are set to install security updates automatically.
- Personnel must not disable security software or install software from untrusted sources.

Security baseline for daily operations

- **Multi-factor authentication** is required on email, source code hosting, hosting and server control panels, domain registrar, marketplace developer portals and any system holding client data.
- **Passwords** are unique for every service, at least 12 characters long, and stored in an approved password manager. Passwords are never shared or sent in plain text.

- **Screen lock** activates automatically after no more than 5 minutes of inactivity, and screens are locked whenever a device is left unattended.
- **Full-disk encryption** (FileVault or BitLocker) is enabled on every laptop and workstation.
- **Clear desk and clear screen:** confidential papers are locked away or shredded, and confidential information is not displayed where others can see it.
- Work is done only on company-approved devices, which are kept up to date. Lost or stolen devices are reported immediately so access can be revoked.
- Personnel receive security awareness guidance on joining and at least annually, including phishing awareness.

Suppliers

We use reputable suppliers for hosting, code hosting and other services, review their security and data protection commitments before use, and grant them only the access they need. Our hosting provider stores our production systems in a data centre in Germany (European Economic Area).

Backups and continuity

- Production data is backed up daily. Backups are access-restricted and retained for a limited period.
- We test restoring from backup at least twice a year.

Compliance and exceptions

Breaches of this policy may lead to disciplinary action or termination of access. Any exception must be approved in writing by the Director, time-limited and recorded.

Report security or privacy concerns through the contact form at skylarksphere.co.uk/#contact (choose “Something else” and start the message with “Security” or “Privacy”), or in writing to our registered office.

Document	Information Security Policy
Organisation	SKYLARK SPHERE LTD (company no. 17031142)
Version	1.0, approved by the Director on 22 September 2026
Review	At least annually, and after any significant incident or change. Next review: September 2027.