SKYLARK SPHERE LTD

Vulnerability and Threat Management Procedure

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

Summary. We keep an inventory of our systems, scan them for known vulnerabilities, apply security updates within set timelines, and accept responsible disclosure reports from anyone.

Asset inventory

We keep an up-to-date list of servers, domains, applications, code repositories, third-party libraries and suppliers that store or process company or client data. Systems not on the list must not hold client data.

Identifying vulnerabilities

- Operating system packages on servers are checked for security updates daily, and security updates are installed automatically (unattended upgrades).
- Application dependencies are checked against published vulnerability databases (for example `composer audit` and `npm audit`) before every release and at least monthly.
- Our websites and applications are scanned externally for common misconfigurations and vulnerabilities at least quarterly, and before major releases.
- We follow security advisories for the frameworks, platforms and services we depend on.

Remediation timelines

Severity (CVSS)	Target time to fix or mitigate
Critical (9.0–10.0), or actively exploited	72 hours
High (7.0–8.9)	14 days
Medium (4.0–6.9)	30 days
Low (0.1–3.9)	90 days, or the next scheduled maintenance

If a fix is not yet available, we apply compensating controls (for example disabling a feature, restricting access or adding firewall rules) and record the risk until the fix is applied. Servers are restarted promptly when a kernel or core update requires it.

Secure development

- Code changes are reviewed before release, and automated tests run on every change.
- Input is validated at trust boundaries, and output is escaped. We use framework protections against injection, cross-site scripting and cross-site request forgery.
- Secrets are kept out of source code and stored in environment configuration.
- Unused services, ports, accounts and software are removed.

Threat monitoring

- Intrusion prevention automatically blocks repeated failed logins to SSH, mail, control panels and web applications.
- Server anti-malware scanning (ClamAV) is installed and running.
- Logs are reviewed for unusual activity, and alerts are investigated under the Incident Response Policy.

Responsible disclosure

We welcome reports of security vulnerabilities. Please report them through our contact form (see security.txt), including enough detail for us to reproduce the issue. We will acknowledge your report within 3 working days, keep you updated, and will not take action against good-faith research that avoids privacy violations, data destruction and service disruption.

Document	Vulnerability and Threat Management Procedure
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.