SKYLARK SPHERE LTD

Access Control Policy

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

Summary. Access to our systems and to personal data is granted only to people who need it for their role, at the lowest level that lets them do the job, and is reviewed regularly and removed promptly when no longer needed.

Principles

- **Least privilege:** users receive the minimum access needed for their current tasks.
- **Need to know:** personal data, including marketplace order and buyer data, is only accessible to personnel who need it to deliver the service to the client.
- **Individual accountability:** every person has their own named account. Shared accounts are not permitted, except for system service accounts owned by the Director.
- **Separation:** administrative access is separate from day-to-day accounts wherever the system allows it.

Granting access

- Access requests are approved by the Director before access is granted, and each approval is recorded.
- Access is granted through role-based permissions in our applications (for example owner, manager and operational roles), so users only see the functions and data their role requires.
- Contractors receive time-limited access that expires at the end of their engagement.

Authentication

- Multi-factor authentication is required for all administrative, hosting, code, email and client-data systems.
- Server administration uses individual SSH keys, administrative server access is restricted to the Director, and repeated failed login attempts are blocked automatically.
- Passwords follow the requirements in the Information Security Policy.

- API credentials and marketplace access tokens are kept only in server-side storage that is not reachable from the internet, are never committed to source code or shared by email or chat, and are only accessible to the application that needs them.

Access to marketplace and client data

- Data received from marketplace APIs on behalf of a seller is only used to provide the service that seller has authorised.
- Seller authorisations can be revoked by the seller at any time. When access is revoked or a contract ends, we stop processing and delete the related tokens and data as described in the Data Protection Policy.
- Production databases are not accessed directly for routine work. Direct access is limited to the Director and is used only for support, maintenance or incident response.

Reviews and removal

- User access to production systems, code repositories and client data is reviewed at least quarterly, and unnecessary access is removed.
- When someone leaves or changes role, their access is removed or adjusted within one working day, and any shared secrets they could have seen are rotated.
- Accounts inactive for 90 days are disabled.

Monitoring

Logins and administrative actions are logged where systems support it. Repeated failed logins trigger automatic blocking. Suspicious access is handled under the Incident Response Policy.

Document	Access Control 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.