SKYLARK SPHERE LTD

Incident Response Policy

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

Summary. This policy defines roles, reporting channels and timelines for handling security incidents and personal data breaches, including how and when we notify affected clients, marketplace partners and regulators.

What counts as an incident

A security incident is any event that threatens the confidentiality, integrity or availability of our systems or data. Examples include unauthorised access, malware, lost or stolen devices, leaked credentials, and data sent to the wrong recipient. A personal data breach is an incident that leads to the accidental or unlawful destruction, loss, alteration, disclosure of, or access to personal data.

Roles and responsibilities

Role	Responsibilities
Incident Lead (Director)	Owns the response, classifies severity, decides on containment, approves and makes all external notifications, and keeps the incident log.
Technical Responder	Investigates, preserves evidence, contains and fixes the issue, and restores services. Assigned by the Incident Lead.
All personnel	Report suspected incidents immediately, and do not investigate alone or delete evidence.

Reporting channels

- **Internal:** personnel report suspected incidents to the Director immediately by phone or direct message, and in any case within 1 hour of noticing them.
- **External:** clients, partners, researchers and members of the public can report through our contact form, as set out in our security.txt, or in writing to our registered office.
- Every report is acknowledged and logged, even if it turns out not to be an incident.

Severity levels

Severity	Description	Target to start response
Critical	Confirmed breach of personal or client data, or a compromise of production systems	Immediately, within 1 hour
High	Likely breach, leaked credentials, or a major outage	Within 4 hours
Medium	Contained malware, or a vulnerability actively targeted with no data impact	Within 1 working day
Low	Suspicious activity with no evidence of impact	Within 3 working days

Response process

- **Identify:** confirm what happened, which systems and data are affected, and whose data is involved.
- **Contain:** isolate affected systems, revoke or rotate credentials and tokens, and block malicious access.
- **Eradicate and recover:** remove the cause, patch vulnerabilities, restore from clean backups, and monitor closely.
- **Notify:** inform affected parties as set out below.
- **Learn:** within 10 working days of closing a High or Critical incident, record the root cause, what worked and the improvements needed, and track those actions to completion.

Notification of breaches

- **Clients and marketplace partners** (such as sellers and the platforms whose APIs we use) are notified without undue delay, and within 24 hours of our confirming a breach affecting their data. We tell them what happened, which data is affected, the likely consequences, what we have done, and who to contact. Updates follow as the investigation progresses.
- **Regulators:** where we are the data controller and the breach is likely to result in a risk to individuals, we notify the UK Information Commissioner's Office within 72 hours of becoming aware of it.
- **Individuals:** where a breach is likely to result in a high risk to individuals, we inform them directly without undue delay, or support the data controller in doing so.
- Where we act as a processor, we assist the data controller with its own notification obligations.

Records

All incidents and breaches are recorded in an incident log with facts, effects, actions taken and notifications made, whether or not notification was required. Records are kept for at least 3 years.

Document	Incident Response 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.