

Business continuity plan

OWNER: AMRIT KHAREL, DIRECTOR, UK OPERATIONS

LAST REVIEWED: SEPTEMBER 2026

NEXT REVIEW: SEPTEMBER 2027

Purpose

This plan sets out how Kyros Software Ltd (Co. 16915277) maintains the continuity of its services in the event of disruption. It is proportionate to a micro software company operating on a remote-first basis.

Scope

This plan covers all business operations, client services, infrastructure and data managed by the company.

Key risks

Risk	Likelihood	Impact	Mitigation
Cloud infrastructure failure	Low	High	Multi-region hosting, automated failover
Data loss or corruption	Low	Critical	Automated backups, offsite replication
Key person unavailability	Medium	High	Documentation, cross-training, succession planning
Cyber security incident	Low	High	Security controls, incident response procedure
Supply chain failure (hosting provider)	Low	Medium	Portable infrastructure, alternative providers identified
Prolonged power/internet outage	Low	Medium	Mobile connectivity, geographically distributed team

Recovery objectives

Metric	Target
Recovery Point Objective (RPO)	24 hours — maximum acceptable data loss
Recovery Time Objective (RTO)	48 hours — maximum acceptable downtime
Maximum tolerable downtime	72 hours

These targets will be verified through a documented test restore of automated daily off-site backups.

Backup strategy

Source code — stored in version control (Git) with remote repositories. Multiple copies maintained automatically.

Client data — automated daily backups with a minimum of 30 days retention. Backups are encrypted and stored in a separate geographic location from the primary data.

Infrastructure configuration — defined as code (infrastructure-as-code) and version controlled, enabling rapid rebuild.

Business records — cloud-based with provider-level redundancy and point-in-time recovery.

Backup testing

Backup restoration is tested at least quarterly to confirm that backups are complete, uncorrupted and can be restored within the target RTO.

Incident response

Detection — monitoring and alerting on all production systems.

Assessment — the Director assesses the nature and severity of the disruption.

Containment — immediate steps to limit the impact (e.g. isolate affected systems).

Communication — notify affected clients, stating the nature of the issue, expected resolution time and any action required on their part.

Recovery — restore services using backups, failover or rebuild as appropriate.

Review — conduct a post-incident review, document lessons learned and update this plan.

Communication plan

Audience	Method	Responsibility	Timeframe
Clients	Email / phone	Director	Within 4 hours of major incident
Staff / contractors	Email / messaging	Director	Immediately
ICO (if personal data breach)	ICO portal	Director	Within 72 hours
Suppliers	Email	Director	As required

Key person risk

As a micro company, key person risk is our most significant continuity concern.

Mitigations:

- All systems, processes and client arrangements are documented.
- Credentials are stored in a shared secrets manager accessible to authorised personnel.
- Infrastructure is automated and can be operated by any competent engineer with access.
- A succession plan is in place identifying who would assume responsibilities in the Director's absence.

Testing

This plan is tested at least annually through:

- Backup restoration drill
- Simulated incident walkthrough
- Review of contact details and access credentials

Test results and any improvements identified are documented.

Review

This plan is reviewed annually or following any significant incident or change to business operations. The next review is due September 2027.