

Backup Policy

ProvisionIQ Ltd — Data Backup, Verification, and Recovery Standards

Document	Backup Policy
Version	1.0
Effective	22 May 2026
Owner	CTO
Review	Annual + on any major infrastructure change
Standards	ISO 27001:2022 A.8.13 · Cyber Essentials Plus · UK GDPR Art. 5(1)(e)

Purpose

Backups are ProvisionIQ's last line of defence against data loss from ransomware, accidental deletion, hardware failure, or disaster. This policy defines what we back up, how often, where we store it, how long we keep it, and how we test it.

Version	Date	Summary
1.0	May 2026	Initial policy

1. Scope

This policy applies to all production data, configuration data, and cryptographic keys held by ProvisionIQ Ltd, including all data processed on behalf of licensed schools, trusts, and local authorities.

2. Backup Schedule

Backup Type	Frequency	Retention Period	Storage Location
Hourly incremental	Every 60 minutes	48 hours	AWS Data Centre UK
Daily full backup	Daily at 02:00 UTC	30 rolling days	Primary + secondary UK facility

Weekly full backup	Every Sunday at 03:00 UTC	13 weeks (3 months)	Secondary UK facility (encrypted)
Monthly snapshot	1st of month at 04:00 UTC	12 months	Secondary UK facility (cold)
Annual archive	31 Dec at 05:00 UTC	3 years	Secondary UK facility (cold, versioned)

3. Backup Standards

Requirement	Standard
Encryption	AES-256 encryption applied before transmission to backup facility. Encryption keys stored separately in approved KMS; never co-located with backup data.
Transmission security	Dedicated secure channel (TLS 1.3) between primary and backup facility. No backup data transmitted over public internet in plaintext.
Integrity verification	SHA-256 hash generated and verified for every backup. Hash mismatches trigger immediate alert to Head of Engineering.
Geographic separation	Primary and backup storage in separate UK data centres; minimum 50 miles apart. Both facilities ISO 27001 certified.
Access control	Backup access restricted to named engineers (minimum two for restore). All access logged immutably. No developer has solo access to production backups.
Immutability	Backups are write-once; once written, they cannot be modified or deleted until the scheduled retention period expires (WORM storage).
Backup of backups	Backup metadata (hash records, job logs) itself backed up daily to a third independent location.

4. Backup Verification and Testing

Test Type	Frequency / Standard
Automated hash verification	Every backup job; immediate alert on failure; Head of Engineering reviews daily
Partial restore test	Weekly: random selection of 5 records restored to isolated test environment; verified for completeness and integrity
Full database restore test	Quarterly: full production database restored to isolated environment; application tested against restored data; RTO measured

DR failover test	Annual: complete platform rebuilt from backup in isolated environment; all features tested; RTO/RPO targets validated
Test documentation	All test results recorded in Backup Test Register; reviewed by CTO quarterly; reported to Board annually

Recovery Targets

Recovery Time Objective (RTO): full platform restoration within 4 hours from a major incident.

Recovery Point Objective (RPO): 1 hour under normal conditions, supported by hourly incremental backups. In the event that local or primary region resources are unavailable, the RPO extends to 24 hours.

These targets are validated by quarterly restore tests. Any test that fails to meet targets triggers an immediate review and infrastructure improvement plan.

5. Backup Access and Security

- Backup systems are isolated from production. A compromise of the production environment cannot directly access backup storage.
- Restore operations require written approval from the Head of Engineering AND one other senior engineer (four-eyes principle for full restores).
- All restore activities are logged immutably with timestamp, authoriser, reason, scope, and outcome.
- Backups are never restored to production following a customer data deletion request, the deletion event is final, and the backup schedule runs its course independently.

6. Backup Deletion

- Backups are automatically deleted at the end of their retention period. Deletion is irreversible (cryptographic erasure).
- When a school's licence ends and pupil data is deleted from live systems, the same data is not restored from backup. Backups containing that data are overwritten as the schedule progresses (within 90 days for all backup tiers).
- Deletion events are logged and confirmation provided to Data Controllers on request.

© ProvisionIQ Ltd 2026. Effective 22 May 2026. Registered in England & Wales, Co. No. 17240497