

BACKUP AND RECOVERY POLICY

Field	Detail
Document reference	POL-BR-002
Version	2.0
Status	Approved
Supersedes	Backup Policy, version 1.x, dated 6 January 2026
Document owner	Chief Technology Officer
Approver	Compliance and QA
Date of issue	22/09/2026
Review cycle	Annually, or on material change to the hosting architecture
Next review due	January 2027
Applies to	MyKnow V5 and MyKnow 365 production environments

1. Overview

This policy defines how Cognisco backs up and restores the data it holds and processes on behalf of its clients, so that information can be recovered in the event of loss, corruption, accidental deletion, or platform failure. It sets out the data stores in scope, the backup mechanism, frequency, and retention applied to each, the arrangements for restore and failover, and the testing that verifies those arrangements work.

The policy supports Cognisco's obligations as a data processor and its information security management system and applies to all production environments hosting client data.

2. Scope

In scope: all Azure services forming part of the MyKnow V5 and MyKnow 365 production environments, and all data held within them, including data processed on behalf of clients.

Out of scope: corporate IT systems and end-user devices, which are covered separately; and non-production environments, which hold no client data and are constructible from source control and infrastructure automation.

3. Roles and responsibilities

Role	Responsibility
Chief Technology Officer	Owns this policy. Responsible for configuring backup, retention, and replication settings in line with this policy, for monitoring backup health, for scheduling and conducting restore and failover testing, and for recording the outcome of each test.
Development team	Responsible for ensuring that any new data store introduced to a production environment is assessed against this policy and configured before it holds client data.
Compliance and QA	Reviews and approves this policy and verifies during internal audit that the configured position matches the position stated here.
Chief Executive Officer	Accountable for business continuity arrangements overall.

4. Data stores in scope

Client data is held in two Azure services only. All other services in the production estate either hold no client data or hold data that is transient or reconstructible and are addressed at section 8.

Data store	Contents	Platform
Azure SQL Database	All structured client data, including assessment, competency, and user records.	MyKnow V5 and MyKnow 365, in separate elastic pools per platform.
Azure Storage	Unstructured client data, including uploaded files and evidence attachments.	MyKnow V5 and MyKnow 365, separate accounts per platform.

5. Azure SQL Database

5.1 Backup

Backups are taken automatically by the Azure SQL platform. No manual backup task is required or performed.

Item	Position
Full backup	Weekly, taken by the platform.
Differential backup	Every 24 hours.
Transaction log backup	Every 5 to 10 minutes.
Point-in-time restore retention	35 days. Applied to all client databases across both platforms.
Long-term retention	Weekly full backup retained for 10 weeks. Applied to all client databases across both platforms.
Backup storage location	Geo-redundant backups are held in Azure-managed backup storage in the United Kingdom. No client data leaves the United Kingdom.

5.2 Replication and failover

Each platform has an Azure SQL auto-failover group configured, with the primary in UK South and the secondary in UK West. Data is replicated continuously to the secondary.

The failover policy is customer managed. Failover is therefore triggered manually by Cognisco and does not occur automatically on loss of the primary region. This is a deliberate choice, so that failover is a controlled decision taken with knowledge of the incident rather than an automatic response to a transient condition.

5.3 Restore

A database can be restored to any point within the point-in-time retention window, or from a long-term retention backup, using the standard Azure SQL restore process. A restore creates a new database; the recovery of service then requires the application to be repointed, or the restored database to be renamed into place.

Individual client databases can be restored independently of one another because tenancy is database-per-client. Restoring one client does not affect any other client.

6. Azure Storage

Item	Position
Redundancy	Geo-redundant storage (GRS). Data is replicated synchronously within the primary region and asynchronously to the paired secondary region.
Failover	Customer-initiated. Failover to the secondary region is triggered manually by Cognisco.
Secondary access	The secondary replica is not readable until failover is performed.
Recovery of individual items	Soft delete allows recovery of deleted items for 31 days.

Because replication to the secondary region is asynchronous, a regional failover may involve the loss of writes not yet replicated at the point of failure.

7. Application platform

7.1 MyKnow V5

Each client instance is hosted as an Azure App Service. Scheduled App Service backups are taken automatically every hour and retained for 30 days. These backups cover application content and configuration; client data itself resides in Azure SQL and Azure Storage and is covered by sections 5 and 6.

7.2 MyKnow 365

The MyKnow 365 application runs in Azure Kubernetes Service. No persistent client data is held in the cluster. Cluster infrastructure is defined as code and provisioned through automated deployment, and container images are held in the container registry

and are rebuildable from source control. The application platform is therefore recovered by redeployment rather than by restoration from backup.

Other services used have been assessed as not requiring backup, because they either do not hold client data or hold derived / copied data from source.

8. Relationship to disaster recovery

This policy governs backup, retention and restore. The replication and failover capability described at sections 5.2 and 6 provides the technical means of recovering from a regional failure, but the procedure for invoking it, the decision authority and the communication steps sit within the disaster recovery arrangements for each platform rather than within this policy.

9. Testing

Restore and failover capability is verified by test rather than assumed. Tests are conducted by the CTO and/or development team and the outcome recorded.

1. A restore test shall be conducted at least annually for each platform, restoring a client database to a point in time and verifying the integrity of the restored data.
2. A failover test shall be conducted at least annually for each platform, exercising the SQL failover group and confirming that the application operates against the secondary region.
3. The date, scope, outcome, and any remedial actions arising from each test shall be recorded.
4. Restores performed operationally, for example to investigate a client support issue, may be recorded as evidence of restore capability where the integrity of the restored data was verified.

10. Recovery objectives

Cognisco's committed recovery time objective or recovery point objective may vary per client contract. The figures below describe the capability the configured arrangements provide and their internal targets.

Scenario	Recovery point	Recovery time
Single database loss or corruption	Within the transaction log backup interval.	Determined by database size; restore creates a new database which must then be brought into service.
Regional failure: SQL	Replication lag at the point of failure.	Determined by manual invocation of failover; failover itself completes in minutes.
Regional failure: Storage	Asynchronous replication lag at the point of failure; unreplicated writes may be lost.	Determined by manual invocation of failover.
Application platform loss	Not applicable; no client data held.	V5: restore of App Service backup or redeployment. 365: redeployment of cluster and services.

Where a client contract commits to a service availability level, availability and recovery are distinct measures and the availability commitment does not imply a recovery objective.

11. Approval

Approved on behalf of Cognisco Limited.

Field	Detail
Prepared by	Chief Technology Officer
Name	Craig Santos
Signature	C Santos
Date	22/09/2026
Approved by	Compliance and QA
Name	Angela Ellis
Signature	<i>A Ellis</i>
Date	22/09/2026

Version history

Version	Date	Author	Summary of change
1.x	6 January 2026	CTO	Previous issue. Covered Azure App Service and Azure SQL for MyKnow V5.
2.0	22 nd September 2026	C Santos	Full revision. Scope extended to MyKnow 365 and to all production data stores. Backup, retention, replication, and failover positions restated to match configuration. Legacy on-premises references and daily manual backup responsibility removed.