Turnkey PI

Back Up Policy

Last Updated 16th September 2025

COMPANY CONFIDENTIAL

Turnkey

Turnkey PI Back Up and Data Recovery Policy

The purpose of this document is to set out the process for backup and restore services for the Turnkey PI application suite.

Applicable Services and Controls

This Policy is applicable to:

- The Turnkey PI SaaS platform including application, database and management servers.
- The Turnkey Insolvency Portal application including application and database servers.

Our Turnkey PI Application suite is currently delivered and maintained by Turnkey's hosting partner, Ekco. The infrastructure is hosted on the Microsoft Azure platform in the UK South region.

Backup Process

Databases are backed up using the backup schedule and retention detailed in the table below.

Backup	Schedule	Retention
Log	Every 10 minutes	14 Days
Daily (Differential)	11:59pm	62 Days
Weekly (Full)	Saturday 11:59pm	365 Days
Monthly	1st of Month	2556 Days (7 years)
Yearly	1st of Jan	3650 Days (10 years)

The Turnkey Insolvency Portal application server is backed up separately to a Recovery Services Vault using Azure Backup. This uses the backup schedule and retention detailed in the table below.

Backup	Schedule	Retention
Turnkey Insolvency Portal	Daily	14 Days

Client and Creditor documents held on the Turnkey Insolvency Portal are now stored on Azure Blob Storage. Production documents are replicated from UK South to UK West. If a client or creditor soft deletes any documents, they are retained for one month only.

Backup Storage Locations

Geo-redundant storage (GRS) is used to store backups. This copies data synchronously three times within a single physical location in the primary region (Azure UK South) using Locally Redundant Storage (LRS). It then copies data asynchronously to a single physical location in the secondary region (Azure UK West). Within the secondary region, data is also copied synchronously three times using LRS.

Backup Encryption

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

Azure Storage encryption is enabled for all storage accounts, including both Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled.

Backup Monitoring

The backup service is provided and monitored by Ekco. All backup jobs are configured to submit tickets to Ekco Support where any warnings or failures are investigated and remediated.

Process for Recovery of Data from Backup

Turnkey will submit a support ticket to Ekco to request a restore.

Client Process for Recovery of Data from Backup

A Turnkey client can submit a support ticket to Turnkey to request a restore. Turnkey will then submit a request to Ekco. For example -

- Request a Data Recovery Form by raising a support ticket with Turnkey.
- Form will require specific details regarding the request and the data involved.
- Turnkey will then raise a support ticket with Ekco.
- Client will be advised of estimated completion date.
- Ekco will restore the data requested to an offline area
- Turnkey will synchronise the offline data from the backup to live database. Client notified once restoration complete.

Timeframe

- An individual case restoration will be carried out within 2 working days.
- A full tenant restore will be carried out within 5 working days.
- Any bespoke restoration of data will be processed as quickly as possible, complexity of the task will determine how long this may take.

A record of physical and logical movement of backup data will be maintained.

Publish Date 16.09.2025
Last Updated 16.09.2025