

# Backup Plan

## Table of Contents

### Introduction

The Backup Plan outlines our organization's strategies and procedures for safeguarding critical data and information assets against loss or corruption. It encompasses a comprehensive approach to data protection, ensuring the availability and integrity of essential business data in the event of unforeseen incidents.

All platform data is currently stored on a MySQL server, so this plan only describes the backup details for this MySQL server and does not address other backup strategies (e.g. for file storage).

### Frequency

Database backups are snapshot-based. A full database snapshot is performed daily. There are no differential backups performed and all snapshot backups are full database backups only.

Transaction log backups occur every five minutes.

### Retention

Daily Backups are retained for up to 7 days. In addition, a weekly snapshot is retained for up to 35 days.

### Encryption

Azure Backup automatically encrypts all backed-up data while storing in the cloud using Azure Storage encryption, which helps meet security and compliance commitments. This data at rest is encrypted using 256-bit AES encryption (one of the strongest block ciphers available that is FIPS 140-2 compliant).

Source:

### Location and Compliance

All backup data is stored in the Azure data center Switzerland North.

This data center complies to CIS Benchmark, CSA STAR Attestation, CSA STAR Certification, CSA STAR Self-Assessment, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, SOC 1, SOC 2, SOC 3, WCAG 2.0, FINMA, CDSA, GxP, PCI DSS, Shared Assessments and TruSight (as of 2024-02-19).

### Restoration

Azure Backup supports Point-in-time restore.

Point-in-time restore is useful in multiple scenarios. For example, when a user accidentally deletes data, drops an important table or database, or if an application accidentally overwrites good data with bad data due to an application defect.

