

# Insendi Data Backup Policy

Version: 1.0

Publication date: 1st November 2019

## 1. Backup of data in database

The backup of data in the database occurs via three methods:

- Data is stored in a PostgreSQL database provided by the Amazon AWS RDS database service. This service provides automated Snapshot backups of the entire PostgreSQL instance not just the database. Such backups occur daily, and happen during a 30 minute period automatically identified as that when the application has least activity,. There is a possibility of slightly lower performance when the backup process commences.
- We also take manual snapshot backups prior to any database migration operations that may occur when the application is upgraded.
- We also use an AWS Lambda Function to automate the copying of backup snapshots from our primary AWS region in Ireland to our secondary region in Germany. This process will occur daily.

In each case the database backup retention period is 30 days.

## 2. Backup of Files

Some parts of the application involve the upload or creation of files that are stored outside of the database. All such files are stored using Amazon S3 which automatically creates a backup copy of each file to an S3 'bucket' in a different region, Germany in our case.

## 3. Full Restoration Testing

Our application is currently mirrored on two AWS availability zones in Ireland. Should one of these data-centres fail then traffic will automatically be directed to the second data-center.

In the unlikely event that the entire Irish AWS region goes down we will restore the application in second Amazon region (Germany) within 3 hours. To this end, we regularly, at least quarterly, recreate the entire application from backup database snapshots and files stored in the second region.

## 4. Monitoring

Our team are automatically notified on the failure of any automated backup operation and will respond accordingly. Should any backup issue result in a failure to backup for more than 48 hours we will notify partners.