Flo Software

Information Security Document

Information Backup and Restore Policy

Version	Date	Description	Author
1.0	4th March 2023	Initial Distribution	Gary Marston

Introduction

Flo Software has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. All data which is backed up must be available for restore in the event of deletion, loss, corruption, damage or any other unforeseen circumstances.

Purpose

The purpose of this policy is to identify and establish procedures and good working practices for the backup and timely restoration of client and Flo Software data.

Scope

The scope of this policy extends to the back-up of all essential information and data regardless of the form it takes on the Flo Software application. Coverage is limited to the cloud-based instances only.

Policy Statement

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice. The following steps will help ensure the clients and Flo's information and data is backed up and restored securely in the most efficient manner possible:

Data Backups

AWS Backup / Restore

1. IT department is responsible for providing system support and data backup tasks are in line with agreed with confirmed Disaster Recovery processes.
2. All IT backup and recovery procedures must be documented, regularly reviewed, and made available to trained personnel who are responsible for performing data and IT system backup and recovery.
3. Wherever practicable, backup media (e.g. tape) must be encrypted and appropriately labelled. Any system used to manage backed-up media should enable storage of date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should be always kept securely with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster.
4. Regular tests must be carried out to establish the effectiveness of the backup and restore procedures by restoring data/software from backup copies and analysing the results.
5. Any data / information no longer in use will be archived in line with any retention policies created via Governance.
6. Flo seeks availability and durability of 99.99% for its backup infrastructure, in line with AWS availability policies.

7. Full instance snapshot backups run daily between 00:00 and 04:00 UTC and have a retention of 7 days.

Data Restores

AWS Backup / Restore

1. Data Restore requests should be created through the IT department service desk application stating
    a. Reason for the restore
    b. Date and time of the backup
    c. Server name for restore.
2. Data restores are treated as whole entities (snapshots), a restore will provide all data at the time of backup.
3. Any restores from cold storage will require a small charge and will have a longer restore eta (2 days max).
4. All backup and recovery (restore) procedures must be documented and made available to Data Centre personnel responsible for carrying out data (file) restores
5. Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen circumstance should be made under the supervision of the IT department via the service ticket tool.
6. Restores to be complete within 6 working hours.
7. The recovery point in time will be as per the backup created between 00:00 and 04:00 UTC.

Data Archiving

1. After a request for client instance shutdown we will archive the data into cold storage for 365 days in line with any retention policies created via Governance.
2. Cold storage archives will be encrypted and stored on availability and durability of 99.99% infrastructure.

Breaches of Policy

Flo will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process and any further training identified for the individual.