HighWire Back-up and Recovery Policy

FUNDS AXIS

Policy title:	Cyber Security Policy: HighWire Back-up and Recovery Policy

Issue	1.2
Approved by:	Darren Burrows
Approval Date:	March 2024
Next Review Date:	March 2025

Scope:	The policy applies to Funds-Axis Group and all contractors and other people working on behalf of the company.
Responsibility for Implementation & Training:	Day to day responsibility for implementation: ISO Day to day responsibility for training: ISO

Distribution methods:	Methods used to communicate this policy: • Information Security Training Module

CONTENTS

FUNDS AXIS

1. Back-up and recovery arrangements

1.1 Background

Our backup and disaster recovery arrangements are designed to ensure high resilience and availability. Through measures such as database snapshots, high-availability setup for servers, Docker containers, and other redundant methods, we mitigate the risk of a single point of failure.

1.2 HighWire Availability

The HighWire service is committed to being available during UK business hours from 6 a.m. to 10 p.m. on weekdays, with the exception of scheduled downtime for new releases. We strive for 99% uptime, except in cases of issues originating from the Wholesaler or its Clients, or other reasons beyond the control of FUNDS-AXIS LIMITED or its partners.

Below is a summary of the arrangements in place for the Production Environment and a summary of how high availability is achieved.

Service	Backup	High-Availability
Application	The application is deployed in AWS ECS Cluster with three standby nodes. ECS will run containers across these instances and auto scale and auto heal whenever required. There is no need of backups at application level.	**Yes (Auto-healing, redundancy)** =3 Standby Servers which will have containers and can auto-scale up to 6 based on requirements Servers =2 Availability Zones (eu-west-1b/eu-west-1c)
Database	**Yes:** Frequency: daily + point in time Retention: 14 days Backup window can be synchronised with clients' FTP uploads. Stored in single region	**Yes (Auto-healing, redundancy)** =2 Database instances (replication) =2 Availability Zones (eu-west-1b/eu-west-1c)
FTP Server	**Yes:** Frequency: daily Retention: 14 days Backup window can be synchronised with clients' FTP uploads. Stored in single region	**Yes (Auto-healing, redundancy)** =3 Servers =2 Availability Zones

FUNDS AXIS

2. RPO / RTO

As part of the HighWire platform, we prioritise achieving stability and robustness in our application delivery. All solution modules are deployed on AWS with configurations for high availability and disaster recovery to ensure resilience.

HighWire is designed and deployed to meet the following recovery objectives:

\ Recovery Point Objective: 8 hours
\ Recovery Time Objective: 24 hours

These objectives represent our commitment to promptly recovering from disruptions to ensure minimal impact on service continuity and data integrity. However, it is worth noting that any issues arising from the Wholesaler or its clients, as well as any other reasons beyond the control of FUNDS-AXIS LIMITED or its partners, may impact these objectives.

3. Backup and Recovery Testing

To validate the effectiveness of our backup and recovery procedures, we conduct comprehensive Backup and Recovery testing every six months. During these tests, we simulate various scenarios to assess the integrity and reliability of our backup systems. Any issues identified during testing are promptly addressed, and resolutions are implemented outside of business hours to minimise disruptions.

4. Disaster Recovery (DR) and Auto-healing Configuration

Our Disaster Recovery (DR) and auto-healing configurations are implemented using AWS services, ensuring rapid failover and service restoration in the event of disruptions. Specifically:

\ DR and auto-healing are configured using auto-scaling groups for all EC2 nodes.
\ Database servers are deployed in a multi-AZ setup with data replication across regions for read-only operations.
\ Failover processes are automated and monitored closely to ensure high availability and data integrity.

5. Communication and Notification Procedures

In the event of a backup or recovery failure, clear communication and notification procedures are followed to ensure timely resolution. This includes:

\ Notifying designated stakeholders promptly.
\ Implementing an escalation process for unresolved issues.
\ Documenting and reporting on the incident and resolution process.
.

END

x

FUNDS AXIS

CONTACT US

📞 +44 (0) 28 9032 9736

✉ info@funds-axis.com

🌐 www.funds-axis.com

📍 12 Gough Square, London,
United Kingdom, EC4A 3DW