

HIGHWIRE


HighWire Back-up and Recovery Policy

FUNDS  AXIS

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

Issue	2.2
Approved by:	Darren Burrows
Approval Date:	May 2025
Next Review Date:	May 2026

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

1. Back-up and Recovery Arrangements	4
1.1 Background	4
1.2 HighWire Availability	4
1.3 Data Protection and Security	4
1.4 Service Availability	4
2. RPO / RTO	6
3. Backup and Recovery Testing	6
4. Disaster Recovery (DR) and Auto-healing Configuration	7
5. Communication and Notification Procedures	7
5.1 Data Access and Return Procedures	7
5.2 Data Recovery Support	7
5.3 Data Authenticity and Integrity Verification	8

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.

Our backup strategy includes daily automated backups of instances created as Amazon Machine Images (AMIs), enabling swift restoration with the latest image. This approach ensures rapid recovery capabilities while maintaining data integrity and security.

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.

1.3 Data Protection and Security

To ensure data integrity and security throughout the backup and recovery process:

- \\ All data is encrypted using:
 - AES-256 encryption for data at rest.
 - TLS 1.2+ for data in transit.
 - AWS Key Management Service (KMS) for encryption key management.
- \\ Access controls include:
 - Role-based access control (RBAC).
 - Multi-factor authentication (MFA).
 - Regular access reviews.
 - Audit logging of all backup and recovery operations.
- \\ Data integrity is maintained through:
 - Automated integrity checks during backup processes.
 - Regular validation of backup data.
 - Checksums verification.
 - Real-time monitoring of backup operations.

1.4 Service Availability

Our backup infrastructure ensures:

- \\ 99.9% uptime commitment.
- \\ Automated failover capabilities.
- \\ Load balancing across multiple availability zones.
- \\ Real-time monitoring via AWS CloudWatch.

- Proactive issue detection and resolution.
- Continuous system health monitoring.

The following table summarises the backup frequencies, retention periods, and high-availability configurations for core infrastructure components hosted on AWS. These details are aligned across both the Business Continuity Plan and the HighWire Backup & Recovery Document.

- Snapshots** are automatically initiated via AWS Backup policies within predefined backup windows.
- All backups are encrypted** and stored across AWS Availability Zones.

Service	Backup Frequency	Retention	Backup Window	High-Availability
Application (EC2)	Not required (immutable infra)	N/A	N/A	Yes (Auto-healing, redundancy). <ul style="list-style-type: none"> 2 Servers. 2 Availability Zones.
Database (RDS)	Daily + Point-in-time recovery	7 days (rolling)	Between 03:00–04:00 UTC	Yes (Auto-healing, redundancy). <ul style="list-style-type: none"> 2 Database instances (replication). 2 Availability Zones.
Analytics Engine (EC2)	Every 12 hours	7 days (rolling)	03:00 & 15:00 UTC	Semi (Auto-healing, no redundancy). <ul style="list-style-type: none"> 1 Server. 1 Availability Zone.
FTP Server	Daily	7 days (rolling)	Between 03:00–04:00 UTC	Yes (Auto-healing, redundancy). <ul style="list-style-type: none"> 2 Servers. 2 Availability Zones.

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, in accordance with our Business Continuity & Disaster Recovery Plan (Section 4):

- \\ **Recovery Point Objective: 12 hours**
This defines the maximum acceptable amount of data loss measured in time. In the event of a disruption, data can be recovered to a point no older than 12 hours prior to the incident.
- \\ **Recovery Time Objective: 3 hours**
This defines the maximum acceptable downtime. HighWire services are expected to be restored within 3 hours of a disruption.

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.

Additional Recovery Provisions:

- \\ Automated recovery procedures for common scenarios
- \\ Regular testing of recovery processes
- \\ Documented escalation procedures
- \\ Clear communication protocols during recovery operations
- \\ Regular validation of recovery time objectives
- \\ Monitoring and reporting of recovery performance

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.

Enhanced Testing Procedures:

- \\ Monthly backup integrity verification.
- \\ Quarterly recovery testing exercises.
- \\ Annual full disaster recovery simulation.
- \\ Regular testing of data accessibility and format compatibility.
- \\ Validation of encryption/decryption processes.

- Testing of data return procedures.

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.

Enhanced Recovery Capabilities:

- Multiple recovery paths for different failure scenarios.
- Automated failback procedures.
- Regular testing of auto-healing mechanisms.
- Continuous monitoring of failover systems.
- Automated system health checks.
- Regular validation of DR procedures.

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.

5.1 Data Access and Return Procedures

In the event of service termination or recovery requirements:

- Data is provided in structured, commonly used formats (e.g., CSV).
- Multiple secure data transfer options available.
- Clear procedures for data access requests.
- Documented data return processes.
- Support for bulk data exports.
- Verification procedures for returned data.

5.2 Data Recovery Support

Recovery support includes:

- \ 24/7 emergency support for critical recovery operations.
- \ Dedicated recovery support team.
- \ Step-by-step recovery guidance.
- \ Documentation of recovery procedures.
- \ Regular updates during recovery operations.
- \ Post-recovery validation support.

5.3 Data Authenticity and Integrity Verification

To ensure data authenticity and integrity:

- \ Digital signatures for backup verification.
- \ Audit trails of all backup and recovery operations.
- \ Chain of custody documentation.
- \ Regular integrity checks.
- \ Version control for all backups.
- \ Secure audit logging.

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