

INTERNAL

Cyber Security Policy Part 2: Funds-Axis Technology Overview

FUNDS  AXIS

Policy title:	Cyber Security Policy Part 2: Funds-Axis Technology Overview
----------------------	--

Issue	1.1
Approved by:	Darren Burrows
Approval Date:	February 2025
Next Review Date:	February 2026

Scope:	The policy applies to Funds-Axis Group and all contractors and other people working on behalf of the company.
Associated documentation:	<ul style="list-style-type: none"> \ All policies \ Funds-Axis Cyber Security Policy: Part 1 Internal Organisation provides an overview of our Internal Organisational arrangements, including organisational responsibility, asset management, access controls, physical and environmental security, device management, incident management etc. \ Funds-Axis Cloud Computing Policy includes details for keeping Customer Data secure on the Cloud. \ Funds-Axis Customer Data Policy details certain specific policies in respect of Customer Data, including in respect of data acquisition, data transmission, processing, storage, archive and destruction.
Responsibility for Implementation & Training:	<p>Day to day responsibility for implementation: ISO</p> <p>Day to day responsibility for training: ISO</p>

Distribution methods:	<p>Methods used to communicate this policy:</p> <ul style="list-style-type: none"> • Information Security Training Module
------------------------------	--

Contents

Our commitment to Information Security	4
Our Technology Architecture	4
Cloud hosting - AWS	4
About AWS	5
Infrastructure as Code	6
Code Management.....	6
Our Technology Stack	7
Core Software	7
Change, Code	7
Server	7
DevOps.....	7
Automated Testing	7
JIRA.....	9
Confluence	9
Sisense Reporting	9
Terraform.....	9
Datadog	9
Data Processing Security	10
Application Security.....	10
Architecture Security	11
Product Development Approach	12
Release Management Framework.....	13
Automated Testing	13
Infrastructure Monitoring	13
Back-up and recovery arrangements	15
HighWire Availability	15
RPO / RTO	17
Back-up and Recovery Testing	19
Help Desk & Support.....	20
Severity Levels:	20
Resolution Time:.....	20

Our commitment to Information Security

As an ISO 9001 and 27001 organisation, the assessment of cyber risk is central to everything we do.

Below are some of the key provisions that we have in place as part of our commitment to managing cyber risk:

- \ HR policies and procedures, including in respect of leavers / joiners;
- \ Information security policies, procedures and training;
- \ Automated transmission and transformation of data to avoid manual process and corruption; and
- \ Secure DevOps practices, including code management and automated testing.

Our Technology Architecture

Our technology architecture encompasses everything you would expect from modern best-of-breed cloud SAAS software.

This includes:

- \ **Cloud hosting**- to achieve High-Availability, Reliability and top security level;
- \ **Secure Data Operations** for data extraction, transformation and load and for storage;
- \ **Infrastructure as Code** - configuration covered and implemented in code. Terraform, Packer and Ansible are our core tools in this area;
- \ **Containers** are used for application deployment;
- \ **Continuous Delivery/Deployment** through use of Continuous Integration/Delivery pipeline;
- \ **Automated Testing**
- \ **Infrastructure and Application Monitoring** and threat detection; and
- \ **Back-up and Disaster Recovery** strategy to ensure resilience and high availability.

Cloud hosting - AWS

We are a cloud-first company. We have selected Amazon AWS as our cloud partner. Our selected data region is Ireland. We use AWS best practices, based on the AWS Well Designed Framework. The AWS services that we utilise include:

- \ **EC2** - Creation of virtual server, underlying infrastructure for ECS cluster.
- \ **IAM** - Security role management.
- \ **RDS** - Relational database.
- \ **VPC** - Underlying networking, designed using security separation principles and deployed in multiple Availability Zones
- \ **ALB** - Application Load Balancer - protects from component failure, offering High Availability.
- \ **S3** - Highly-scalable storage.
- \ **Route 53** - Controlling and managing our domains.
- \ **Certificate Manager** - Providing our SSL security to our applications.
- \ **Lambda** - Automating tasks for our servers.
- \ **CloudWatch** - Logging statistical data for detection of errors

About AWS

AWS is designed to be the most flexible and secure cloud computing environment available today. The AWS core infrastructure is built to satisfy the security requirements for the military, global banks, and other high-sensitivity organizations. This is backed by a deep set of cloud security tools, with 230 security, compliance, and governance services and features.

AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. AWS supports 90 security standards and compliance certifications, and all 117 AWS services that store customer data offer the ability to encrypt those data.

For more information on AWS and Cloud security can be found at the following links

- \ <https://aws.amazon.com/what-is-aws/>
- \ https://aws.amazon.com/about-aws/global-infrastructure/?pg=WIAWS-N&tile=learn_more
- \ https://aws.amazon.com/security/?nc1=f_cc

Infrastructure as Code

Below is a summary of our infrastructure-as-code and code management arrangements:

- \\ **Application** - tested code builds are packaged in Docker images and then deployed into AWS ECS cluster. The same build artefacts are used for all environments to let us test the same version of application, only changing runtime configuration specific to the environment.
- \\ **Database** - we use tools like Liquibase to manage and version database schema changes/migrations;
- \\ **Infrastructure** - All our infrastructure configuration is covered and implemented in code, and have all our infrastructure code implemented in technologies like Terraform, Packer, Ansible; and
- \\ **Deployment** – Our technologies our deployed using Jenkins, which will perform all the build operations for our Applications, Databases, and Infrastructure.

Code Management

Source Code is stored in Atlassian BitBucket. (<https://bitbucket.org/>).

Bitbucket Cloud is a Git based code hosting and collaboration tool, built for teams. Bitbucket's best-in-class Jira and Trello integrations are designed to bring the entire software team together to execute on a project. It provides one place for the team to collaborate on code from concept to Cloud, build quality code through automated testing, and deploy code with confidence.

Reference: <https://bitbucket.org/product/guides/getting-started/overview>

Branches will be created against each User story in Jira. Based on these branches, code check-in and Pull Requests are created.

Our Technology Stack

Below is a summary of our technology stack.

Core Software



Change, Code



Server



DevOps



Automated Testing



Category		Tools / Technology / Practice
1	Front End:	
	Programming Languages	HTML 5, CSS 3, Javascript
	Framework	Vue, Vuex,
	Build Tools	Node.js, npm
	Testing Tools	Cypress
2	Back End:	
	Programming Languages	Java,
	Framework	Spring
	Build Tools	Maven
	Testing Tools	Rest Assured, Junit, Cucumber, Mockito
3	Database	
	Database	PostgreSQL (AWS RDS)
	Schema Versioning	Liquibase
4	Business Intelligence	
	Business Intelligence	Sisense
5	DevOps	
	Core Tools	AWS, AWS ECS, AWS Lambda, Terraform
	Operating System	Linux, Windows
	Monitoring	Datadog
6	Testing	
	Methods	Unit Testing, Integration Testing
		E2E Testing, Exploratory Testing,
		Automated Testing, API Testing
7	Others / General	
	Issue Tracker	Jira
	Document Maintenance	Confluence
	Source Code Repository	BitBucket
	Continuous Delivery and Deployment	Jenkins
	Docker	Virtualize software in container
	Docker Compose	Run Multi docker applications
	Swagger	API Verification and Testing

JIRA

JIRA is an Incident Management Tool used for Project Management, Bug Tracking, Issue Tracking and Workflow. JIRA is based on the following three concepts – Project, Issue and Workflow. JIRA is developed by Atlassian Inc., an Australian Company.

Reference: <https://www.atlassian.com/software/jira/guides/getting-started/overview>

Confluence

Confluence is a collaboration wiki tool used to help teams to collaborate and share knowledge efficiently. With confluence, we can capture project requirements, assign tasks to specific users, and manage several calendars at once with the help of Team Calendars add-on.

Reference: <https://www.atlassian.com/software/confluence>
<https://confluence.atlassian.com/confeval/confluence-evaluator-resources/confluence-features-functions>

Sisense Reporting

Sisense is an agile business intelligence (BI) solution that provides advanced tools to manage and support business data with analytics, visuals, and reporting.

Reference: <https://www.sisense.com/en-gb/support/>
<https://documentation.sisense.com/latest/administration/embedded-analytics/rebranding-sisense/white-label.htm>

Terraform

Terraform is a tool for building, changing, and versioning infrastructure safely and efficiently. Terraform can manage existing and popular service providers as well as custom in-house solutions. Configuration files describe to Terraform the components needed to run a single application or an entire data centre. Terraform generates an execution plan describing what it will do to reach the desired state, and then executes it to build the described infrastructure. As the configuration changes, Terraform is able to determine what changed and create incremental execution plans which can be applied.

The infrastructure Terraform can manage includes low-level components such as compute instances, storage, and networking, as well as high-level components such as DNS entries, SaaS features, etc.

Reference: <https://www.terraform.io/>

Datadog

Datadog is an essential monitoring platform for cloud applications. Datadog brings together data from servers, containers, databases, and third-party services to make the stack entirely observable.

These capabilities help the DevOps team to avoid downtime, resolve performance issues, and ensure customers are getting the best user experience.

Providing beautiful visual displays of system statistics, allowing for the DevOps team to track anomalies in server activity and identify peak times.

Reference: <https://www.datadoghq.com/>

Data Processing Security

Our client operations involve a large amount of data transfer and storage.

We ensure secure data transmission and storage, including through:

- ▮ Robotic process automation, removing the need for manual interventions;
- ▮ Data receipt through secure sFTP and ETL tools;
- ▮ Encryption of data in transit - all communication to our application is encrypted using strong SSL certificates; and
- ▮ Encryption at rest

Protocols for secure connections

We use ELBSecurityPolicy-2016-08 in our ELB which uses TLS both within the application and also for email communication. This can be seen from the fact that the URL starts with "https," and there's an indicator with a padlock telling you the connection is secure.

Accessibility via approved and secure ports and services

We use ELB and Security Group Policies to disable access to ports unnecessary to the use of the application.

Encryption at Rest

The RDS is configured with encryption keys managed by AWS Key Management Service (KMS). We are using a symmetric 256-bit encryption key that never leaves AWS KMS unencrypted. It is configured with the key specification "SYMMETRIC_DEFAULT", which encrypts the data using the algorithm AES-256-GCM.

Application Security

Key features of application security include:

- ▮ Users authentication - we follow OWASP best practices for the authentication standards;
- ▮ User log-in security - our application uses password requirements recommended by OWASP;
- ▮ Secure password storage - we use secure BCrypt password hashing algorithm with multiple hashing iterations and salt generated each time the password is generated;
- ▮ IP restrictions - we can restrict login to the application using IP whitelisting;
- ▮ Auto-generated email notifications – instant awareness of repeated, invalid, access requests; and
- ▮ Activity / log-in monitoring - we log all activity in the application.

Password Requirements

The Password Strength requirements are as follows: -

- ▮ field should be minimum 10 characters long

- field should be maximum 256 characters long
- field must contain at least 1 uppercase character (A-Z)
- field must contain at least 1 lowercase character (a-z)
- field must contain at least 1 digit character (0-9)

We use TLS - SHA256 Hash functions. Passwords are saved in a hashed form with cryptographically-strong random salt using BCrypt. Salt is generated each time the password is generated.

Architecture Security

- Activity / log-in monitoring - we log activity in the application.
- Threats detection & analysis - We use log analysis and infrastructure monitoring software (DataDog) to detect security threats and potential abusive behaviour in our application.
- Multifactor Authentication (MFA) is required to access our internal systems such as code repository.
- Access to management services is restricted using IP whitelisting.
- Complete separation of client data utilising individual S3 storage pathway

Logging

The system will record the login success and failures of the users, we also record the changes made to the database.

Product Development Approach

We follow an agile approach to product development. This includes through the use of JIRA to document user stories and the performance of testing against those user stories. User stories are assigned to a development sprint, with each development sprint is a maximum of 2-weeks.

We do not perform bespoke product developments. All developments are released to the core product. Product Developments are informed and shaped by regulatory change, our client user group, user feedback and features request.

Release Management Framework

Our release management framework is characterised by the use of continuous integration pipelines and automated testing.

Releases are planned to take place outside of business hours (8.00am – 10pm GMT).

For full details see the document “Funds-Axis HighWire Release Management Framework”

Automated Testing

Our priority is to have the highest possible level of coverage for automated tests.

Our use of automated testing covers the following:

Test Approach	Overview
Unit testing	We write unit tests for Backend (JUnit) and Frontend (Jest).
Integration testing	We use REST Assured in combination with Cucumber for API (backend) BDD tests and Cypress for Frontend.
End-to-end testing	E2E tests are based on BDD methodology with Cypress and Cucumber as underlying technologies.
Exploratory Testing	For final confirmation that all required functionalities are performing as expected.
Automated code quality review	SonarQube is used to perform automated testing of code quality. It checks code Quality and reviews to detect bugs, code smells, and security vulnerabilities.

To track quality metrics of the application we use SonarQube that collects code metrics, tests metrics, technical debt charts etc. In addition to the above, we also make use of:

- Manual code reviews
- Manual user testing versus Jira User stories.

Infrastructure Monitoring

Datadog is used for cloud infrastructure monitoring.

This includes for AWS, Docker, performance monitoring, site availability, log analysis, server monitoring and alerting, including in respect of memory usage, back-ups, CPU usage etc.

Currently, we work on three environments - local, staging and production and automated deployments are done up to production environment.

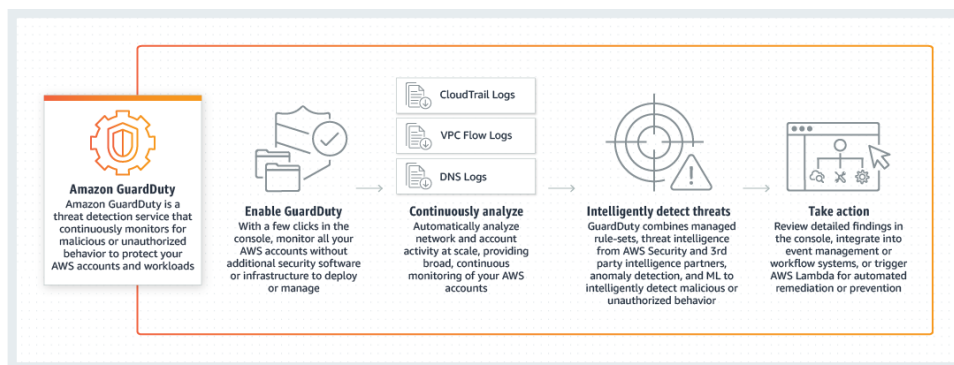
Datadog Host Map:



AWS Guard Duty

We also make use of AWS Guard duty which is a threat/anomaly detection tool. It provides a central security location for monitoring and providing a detailed alert on anything it detects. It's a detection system that makes use of machine learning for analysing all the log data in our AWS account from sources like CloudWatch, providing continuous threat detection

This is integrated with DataDog so we can continue to view all these alerts/monitoring data in one single location. In some cases, AWS Guard Duty perform automated remediation actions, using a combination of CloudWatch and Lambda functions.



DDoS Protection

AWS benefits from protections of AWS Shield Standard. This is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

Back-up and recovery arrangements

Our Back-up and Disaster Recovery arrangements are designed to ensure resilience and high availability. This includes through, database snapshots, High-Availability setup for servers, Docker containers etc, with an objective of avoiding a Single Point of Failure.

HighWire Availability

Apart from scheduled downtime planned for new releases, the HighWire Service is designed to be available 365 days a year, 24 hours a day for not less than 99.5% of the time except for:

- └ any problems coming from the Wholesaler or its Clients;
- └ any other reasons beyond the control of FUNDS-AXIS LIMITED or its partners.

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

Service	Backup	High-Availability
Application	Not required due to immutable infrastructure.	Yes (Auto-healing, redundancy) =2 Servers =2 Availability Zones
Database	Yes: Frequency: daily + point in time Retention: 30 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
Sisense	Yes: Frequency: 12hrs Retention: 30 days Stored in single region	Semi (auto-healing, no redundancy) =1 Server =1 Availability Zone
FTP Server	Yes: Frequency: daily Retention: 30 days Backup window can be synchronised with clients' FTP uploads. Stored in single region	Yes (Auto-healing, redundancy) =2 Servers =2 Availability Zones

	<p>Yes:</p> <p>Frequency: 12hrs Retention: 30 days Stored in single region</p>	<p>Semi (auto-healing, no redundancy)</p> <p>=1 Server =1 Availability Zone</p>
--	---	--

RPO / RTO

Based on the above, we work to the following Recovery Point objectives and Recovery Time Objectives, for specified business continuity events.

	Scenario	What happens?	RTO	RPO
1	Sisense EC2 instance crashed.	Access to Sisense is unavailable. Sisense EC2 instance is automatically re-created (possible in another, healthy AZ). Sisense instance data is based on last backup. Access to Sisense is recovered	<1hr	max. 12 hrs
2	Application EC2 instance crashed.	Part of traffic to application may throw failures during load balancer traffic switching. Application EC2 instance is automatically re-created (possible in another, healthy AZ). Load balancer starts seeing instance as healthy and routing traffic to it.	<1min	0
3	Primary instance of database crashed.	Users starts seeing failures in requests to application (don't get data) Failover to standby database. Users starts receiving data from secondary database.	<5min	0
4	Bug in application caused removal of users' data.	Users see wrong data in the application. We manually start RDS snapshot restore procedure to point in time with latest correct data.	<12hrs	Depends on the duration of having wrong code in application.
5	Single availability zone is down.	Sisense: see scenario 1. Application: see scenario 2. Database: see scenario 3.	<1hr	max. 12 hrs
6	Two availability zones are down.	Total outage of the platform (see AWS region failure scenario)	(as in 7)	(as in 7)
7	Single AWS region is down	Total outage of the platform.	Depends on AWS recovery. Should be <24hr	Depends on AWS (if they also loose data we end up with no backups)

9	Sisense batch build failure	Data from the daily Sisense build is unavailable in the application at the scheduled time. We need to troubleshoot the origin of the error and resolve it. Re-run the batch build before the next schedule starts.	<2hr	Depends on what batch builds have failed.
10	Easymorph batch build failure	A batch build fails due to an error. We need to troubleshoot the origin of the error and resolve it. Re-run the batch build before the next scheduled Sisense batch build starts.	<1hr	0
11	FTP data lost	A bug has caused all the FTP data to be wiped. Manually recover the data using the AWS Backup of the EFS.	<1hr	24hrs

Back-up and Recovery Testing

Testing of Backup and Recovery will happen at the end of each month.

EC2 Instance:

Step	Task
1.	Create a cloned instance of an existing production server using an AMI.
2.	Restore a previous day snapshot to the cloned instance.
3.	Test that the cloned instance with the newly recovered snapshot is functioning correctly.
4.	Perform integrity and error check, and record any errors found.
5.	Connect to a cloned RDS Database if applicable.
6.	Test that the data is accessible, modifiable, and removable.
7.	Record results and any errors found.
8.	Run through test simulations and record results.
9.	Destroy cloned instance.

RDS Database:

Step	Task
1.	Restore the snapshot of the RDS database with a different identifier
2.	Access the database to confirm it is working.
3.	Test that the data is accessible, modifiable, and removable.
4.	Perform integrity and error checking on the database, and record any errors found.
5.	Run through test simulations and record results.
6.	Destroy the restored RDS database instance.

If integrity or errors occur, then begin testing the live environments for the same problems and begin repair operations outside of business hours, if required.

Help Desk & Support

Support Service will be provided between 7 a.m. UK time to 5 p.m. UK time for European customers and until 7pm U.S. EST time for US Customers (17 HOURS, 5 DAYS PER WEEK).

Help-desk tickets are raised by clients, directly through the application.

We will address support issues that can be reproduced by us in accordance with the severity levels defined below. The severity level assigned to support issues will be jointly agreed between the Customers and us.


Enhancement requests and/or modifications are not considered as support issues and do not have any associated severity level.

Severity Levels:

- (i) Severity Level 1 - means a critical issue which will be responded to in 30 minutes.
A critical issue occurs when system users are unable to access or successfully log in to HighWire. This would include when there is a complete loss of HighWire Services or errors within the application that are preventing access or use of the services. Known or suspected security breaches are also within this category;
- (ii) Severity Level 2 - means a business impacting issue which will be responded to in 2 hours. The Wholesaler or its Client is unable to perform a non-mission critical business function and high business impact occurs, or there is an underperforming workaround in place for a mission critical business function;
- (iii) Severity Level 3 - means delayed performance and will be responded to in 8 hours.
Process or calculation slowdown that impacts on the efficiency of the Wholesaler or its Clients' normal business operations;
- (iv) Severity Level 4 - means cosmetic problems and will be responded to in 24 hours; Minor flaws that do not impact the Wholesaler or Clients' normal business operations.

Resolution Time:

Technical support issues meeting the severity level descriptions set forth above will be addressed as set forth below:

-  Severity Level 1 – FUNDS-AXIS LIMITED development or support resources will work 24 hours per day, 7 days per week, to resolve all Severity Level 1 incidents until the issue has a temporary repair or workaround in place. A permanent repair will be performed during business hours. Upon request by FUNDS-AXIS LIMITED, the Wholesaler will use all reasonable efforts to make a designated contact available 24 hours per day, 7 days per week to assist FUNDS-AXIS LIMITED development or support resources in the investigation of the issue;

- Severity Level 2 – FUNDS-AXIS LIMITED development or support resources will work extended business hours to resolve all severity level 2 incidents until the issue has a temporary repair or workaround in place. A permanent repair will be performed during business hours;
- Severity Level 3 – FUNDS-AXIS LIMITED development or support resources will work during business hours until a temporary repair or workaround is in place and then work to provide a permanent repair;
- Severity Level 4 – FUNDS-AXIS LIMITED development or support resources will work during business hours to resolve severity level 4 incidents in order of their priority.



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