

INTERNAL

Cyber Security Policy

Part 1: Internal Organisation

Policy title:	Cyber Security Policy: Part 1 Internal Organisation
Issue	8.0
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 2: Funds-Axis Technology Overview provides an overview of our policies in respect of technology management, including data security, encryption, passwords, SDLC, Back-up, Recovery 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

1. Introduction..... **Error! No bookmark name given.**

2. Business Overview **Error! No bookmark name given.**

3. Roles & Responsibilities **Error! No bookmark name given.**

4. Organisation of Information Security **Error! No bookmark name given.**

5. Information Classification and Handling..... **Error! No bookmark name given.**

6. Human Resource Security..... **Error! No bookmark name given.**

7. Asset Management..... **Error! No bookmark name given.**

8. Access Control..... **Error! No bookmark name given.**

9. Physical & Environmental Security **Error! No bookmark name given.**

10. Operations Security **Error! No bookmark name given.**

11. Network Security and Device Management..... **Error! No bookmark name given.**

12. Communications Security..... **Error! No bookmark name given.**

13. Supplier Relationships **Error! No bookmark name given.**

14. Information Security Incident Management..... **Error! No bookmark name given.**

15. Business Continuity and System Availability..... **Error! No bookmark name given.**

16. Contact with Regulatory Authorities and Special Interested Groups... **Error! No bookmark name given.**

17. Information Security in Project Management..... **Error! No bookmark name given.**

18. Compliance and Information Security Monitoring & Review **Error! No bookmark name given.**

1. Introduction

Funds-Axis is a technology-based business which involves the processing, management and transfer of a large amount of client and other data on a daily basis. Given the nature and structure of the business, the company is dependent on the smooth, uninterrupted, and secure operation of its Information Technology platform and has a heavy dependency on certain key technology suppliers to this end.

This policy is shared with or made available to relevant interested parties upon request as detailed in the Interested Parties Register in the Context and Scope document.

1.1 Scope

This policy applies to all information, information systems, networks, applications, locations and users of Funds-Axis Ltd or supplied under contract to it. It provides an overview of our Internal Organisational arrangements, including organisational responsibility, Asset Management, access controls, physical and environmental security, device management, incident management etc.

Separate policy documents are available in respect of the following:

- \\ **Funds-Axis Cyber Security Policy: Part 1 Internal Organisation**
- \\ **Funds-Axis Cyber Security Policy Part 2: Funds-Axis Technology Overview** provides an overview of our policies in respect of technology management, including data security, encryption, passwords, SDLC, Back-up, Recovery 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.

Collectively, these documents are referred to as Funds-Axis Information Security and Technology Controls, "IS&TC".

1.2 Objectives

This policy sets out the company's overall plan and procedures for the management and control of these activities including the company's Information Security Management System (ISMS). The ISMS is designed to ensure information held and managed by the company and its IT systems are managed effectively in the following main areas:

- \\ Security
- \\ Availability
- \\ Processing Integrity
- \\ Confidentiality

Effective management of this activity is critical to the day-to-day operations of the company and its ultimate success for several reasons:

1. Business continuity
2. Client requirements
3. Legal and regulatory requirements

1.3 Policy Aim

The aim of this policy is to establish and maintain the security, availability, processing integrity and confidentiality of information, information systems, applications and networks owned or held by the company by

- ✓ Describing the principles of information security and explaining how they are implemented in the organisation.
- ✓ Introducing a consistent approach to information security, ensuring that all members of staff fully understand their own responsibilities.
- ✓ Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- ✓ Protecting information assets under the control of the organisation
- ✓ Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.

We are committed to satisfying all interested party and regulatory requirements related to information security and continually improving our information security processes.

All employees have involvement with information and IT systems and accordingly have responsibilities for information security and technology controls. This policy sets out those different responsibilities and after reading this policy, employees should understand the importance of information security and IT controls in the context of the Funds-Axis business and their role in ensuring the company maintains effective control over information and IT security.

1.4 Key Information Security Risks

The material risks in terms of our physical and information security and the related key controls are described in the Quality and Information Security Risk Registers.

2. Business Overview

2.1 Business Locations and Boundaries

Funds-Axis operates from two office locations, one in Belfast, Northern Ireland, and one in Chennai, India.

Address

4A Weaver's Court Business Park
Linfield Road
Belfast
BT12 5GH

No.158, Gulecha Towers,
Arcot Road,
Opposite Forum Mall
Vadapalani - 600 026





There is no physical server at either location, instead we utilize the Microsoft 365 Sharepoint Collaboration Portal.

2.2 Work from Home

Our policy, including in response to the coronavirus pandemic, is to facilitate work from home (WHF) arrangements.

This is enabled by our cloud-based technology infrastructure, as described in this document.

However, we recognize that working from home poses new and additional information security risks, including:

-  Levels of wifi connectivity
-  Disposal of confidential waste
-  The risk of theft of a machine
-  The home working environment can mean that screens, documents, and work-related conversations can become available to family members and other cohabiters. So, staff will need guidance on how to organise their work and the risks associated with the data they handle.

Particularly for staff in Chennai there are also issues in regard to uninterrupted power supply etc.

To address these issues,

- Our **Network Security and Device Management Policy** at Part 11 is designed to support remote working;
- An inventory is retained of all staff and the assessment of the satisfactoriness of the WFH arrangements, the physical environment, the time criticality of their roles, the sensitivity of data that they have access to, and their printing requirements;
- A review of each team member's WFH arrangements are confirmed as part of the recruitment process, and on at least annual basis thereafter (see below);
- Physical office locations are retained and made available to staff;
- Those who do not have suitable WFH arrangements for the roles that they are required to perform are required to make use of the physical office locations. In the event that the physical office location is not available (e.g. because of coronavirus lock-down), then the staff member's role will be reviewed and duties reallocated as appropriate;
- The use of Teams messaging is encouraged;
- Staff are provided with screen protectors so that the content of their screens is not visible to others;
- Where staff do require to print sensitive or confidential data, then shredding machines or confidential paper bins, plus disposal arrangements are put in place; and
- We push for a digital only approach so that there is no requirement for printing and we do not provide printers;
- Staff are provided with headsets to assist in ensuring conversations are kept confidential where possible

Also,

- We invest in automation to reduce (with a target of zero) the manual involvement in downloading or uploading of data; and
- Data flows documentation is in place in respect of all data flows to identify opportunities for further improvement.

Additionally, training is provided to all staff in respect of work from home arrangements, including in respect of information security and health and safety etc.

Review of work from home arrangements

This includes through discussions with staff, use of questionnaires and also video based assessment of work conditions - to confirm that:

- \\ The team member is able to work in a secure private space;
- \\ Meetings and calls, including video calls can be held in private; and
- \\ Machine is secure from theft.

2.3 Main Business Activities and IT Infrastructure

The company's main activities are

1. Investment Compliance, Regulatory Reporting and Shareholder Disclosures Services addressing client regulatory compliance and disclosure requirements provided through the Funds-Axis software application
2. Information Portals (Global Exchanges, Global Disclosures and Atlas) – online portals providing information and updates on various Stock Exchanges and Shareholder Disclosure requirements around the world and
3. Related Consultancy and Training Services

The data flows and the related IT environment for these activities are summarized below.

Business Area and Data Flows	Main IS&TC Issues
<p>Funds-Axis Compliance monitoring services</p> <p>On a daily basis client data (investment fund holding data) will be downloaded onto local machines for investment holdings file preparation prior to uploading to client Funds-Axis applications. These applications are supported internally and are hosted on the AWS Platform.</p> <p>Client data inflows into our networks come via:</p> <ul style="list-style-type: none"> \\ FTP/Secure-FTP transfer or download from secure client portal direct onto the collaboration portal \\ Email, where it will be both on our Microsoft exchange hosted server and on the collaboration portal <p>Once uploaded to client Funds-Axis applications, daily processing occurs, and investment compliance and other results are generated. The Funds-Axis applications are cloud based and can be accessed</p>	<p>The main direct concern for the company is the secure handling and storage of downloaded client data, processed reports, and other outputs as part of Funds-Axis daily processes.</p> <p>Given the daily business critical nature of certain of the company's service offerings, ensuring continuity of service is a further key concern.</p>

from anywhere in the world and data can be downloaded. Access is subject to username and password restrictions and there is the potential for restricted I.P. address access. Reports and other outputs may then be assembled and sent to clients.

The investment compliance and disclosures reporting services are daily business critical activities for clients and the company's Business Continuity and Disaster Recovery Policy and procedures reflect this.

Global Disclosures.com and Global Exchanges.com portals Atlas portal

These are online information portal services run on web-based portals provided and maintained by AWS. These portals can for the most part be maintained online from any computer anywhere in the world.

Client access to the portals is by username and password control.

Staff access to the Portals for update of content is controlled through the Company Access Control Matrix.

The main IS&TC risks relate to the content, operation of the portals and hosting arrangements.

The management of the supplier relationship is detailed at the Supplier Relationships section of this policy.

Consultancy and Training

Consultancy and training for Investment Compliance and Regulatory reporting are delivered in client offices, remotely or from training and conference venues.

Relevant data is stored centrally, backed-up and is recoverable. Hard copies are retained in secure locked filing cabinets.

The key Information Security risks relate to the loss of documents and records, which are mainly company assets.

2.4 Other ancillary business IT infrastructure

All of Funds-Axis key internal business systems are cloud-based third-party systems.

All the Company's IT systems are fully listed in the Access Control Matrix. This includes:

- \\ Identification of the tool
- \\ Billing arrangements (to ensure continuity)
- \\ Classification of the data that is held on the systems (e.g. client vs. internal data and sensitivity)
- \\ Whether it is accessible only via VPN or IP address restriction
- \\ Whether multi-factor is implemented.

As a policy, we user access is based on a “least privileges required” model where user access and permissions is limited in respect of both the tasks they can perform and the portfolios that they have access to.

We also utilise multi-factor and with the implementation of VPN, IP restrictions or MFA where available.

User access and privileged access to the different systems and applications is controlled in line with user role and requirements.

3. Roles & Responsibilities

3.1 Board

The Board of Directors has overall responsibility for IS&TC within the Company. This responsibility is discharged as set out below.

3.2 Information Security Roles and Responsibilities

Internal Information Security roles and responsibilities are clearly defined in this IS&TC Policy and cover all aspects of

- policy review, update, and approval,
- reporting framework for and monitoring of IS&TC performance,
- controls testing and reporting on compliance

The responsibilities of key suppliers are also clearly documented and understood through

- Contracts, Agreements, and detailed Service Level Agreements as detailed at Section 13.
- Regular service meetings and reviews to deal with operational performance issues

3.3 Segregation of Duties

Key responsibilities are split between the:

- The Board of Directors,
- The Information Security Officer (ISO)
- The Customer Data Officer
- The Cloud Computing Officer
- Line Managers, and
- Individual users

This provides an appropriate level of segregation of duties as between users of information systems and those responsible for monitoring and testing of controls and compliance.

3.4 IS&TC Policy and Risk Management Framework

The Policy sets out the company's overall plan, high level procedures and risk management framework for IS&TC. The CEO reviews and approves this Policy annually as well as approving any amendments which may be made in the interim. This and other policy and procedure document reviews and updates are controlled via the Company Policy & Procedures Review and Approval Log.

The Board also considers the overall results of Controls Testing, business, legal, regulatory, and other developments throughout the year to ensure the Policy and overall Risk Management Framework remain relevant to the developing needs of the business.

Relevant risks and compliance with policy are managed through the Information Security and Quality Risk Registers. This links to a programme of monitoring and regular testing of controls to ensure that management and the Board have visibility on the operational effectiveness of the ISMS and that updates, and corrective actions are taken as required.

Results of the testing are reviewed by the ISO with reporting to senior management and / or the Board in line with this policy.

Independent assurance on the operation of the ISMS is provided through outsourced Internal Auditing and Consultancy. The company also plans to obtain formal Controls Certification by external audit firms during the current financial year.

3.5 Information Security Officer (ISO)

The ISO role has overall responsibility for the implementation, running and regular review of the ISMS as follows:

- ✓ To receive the relevant reports and assurance from the Customer Data Officer, the Cloud Computing Officer, Customer Data Officer, Line Managers and Individuals
- ✓ To provide the Board of Directors with relevant reports and Assurance
- ✓ ensuring the detailed procedures and controls making up the Risk Assessment and Controls Framework remain relevant, up-to-date, and fully aligned to the IS&TC Policy
- ✓ monitoring and reporting on controls testing results to ensure Board and management visibility of risk management issues and revision or update of policy, procedures, controls, or controls testing as required by the changing business environment
- ✓ Liaison with external assurance providers.

The ISO has day-to-day responsibility for the following areas:

- ✓ ensuring the effective operation of the audit testing programme and retention of satisfactory audit evidence for internal and external audit purposes

Responsibility for specific key control areas including

- IT Asset Register maintenance
- IT Access Control Matrix maintenance
- Procurement and Decommissioning of IT assets
- IS&TC aspects of Joiner / Leaver Process
- Incident Management Reporting and follow-up
- Policy & Procedure Review and Approval Logs

3.6 The Customer Data Officer

The Customer Data Officer is a Team Member with assigned responsibilities in respect of ensuring the Customer's data journey with Funds-Axis, including data transmission, processing, storage, archive and destruction is in compliance with Customer Data Policy.

3.7 The Cloud Computing Officer




As regards solutions made available to Customers, Funds-Axis deploys its proprietary technology and other third-party components on “*physical cloud computing infrastructure*” (PCCI) provided by a third party. The PCCIP makes available a “Client interface”, which is the software layer made available by the *Cloud computing service provider* which Funds-Axis uses to manage the *Cloud computing resources* and which include, for example, tools to trace users' access, tools to provide metrics for implemented security settings, lists of users with access to data and systems, and so on.

Funds-Axis is the “*Resource Operator*” of the PCCI and the *Signatory* to the contract with the PCCIP. The “*Cloud Officer*”, is responsible for the use of cloud services and shall guarantee the competences of the staff managing *cloud computing resources*.

This is further described in our Cloud Computing Policy.

3.8 Line Managers / Team Leaders

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

-  The information security policies applicable in their work areas
-  Their personal responsibilities for information security
-  How to access advice on information security matters

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

They are also responsible for ensuring that mandatory IS&TC Training is completed by their permanent and temporary staff, together with ensuring that staff are competent.

Any breaches of policy must be reported to their Line Manager or the ISO immediately and appropriate corrective action taken including disciplinary action, if required. Any such breaches or significant audit testing findings are discussed and considered as part of the individual's annual appraisal.

3.9 All Staff

Individual staff members are responsible for ensuring that they comply with information security procedures. Failure to do so may result in disciplinary action.

Staff must complete company mandatory Information Security Training and Testing which is scheduled for them.

Where specific roles have increased training and qualification requirements it is the employee's responsibility to complete these and maintain the qualifications and any continuing professional development qualifications, as required.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity, and availability of the information they use is maintained to the highest standard.

See also under Part 11 on Network Security and Device Management.

3.10 External Contractors

Contracts/NDAs with external contractors and suppliers that allow access to the organisation's information systems are to be in operation before access is allowed. These Contracts/NDAs will ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4. Organisation of Information Security

4.1 Physical Organisation

The Company's physical locations are in Belfast and in Chennai. There are various physical and environmental and other controls in place to protect IT assets and information. These are detailed further in the relevant sections of this policy and summarized below.

Physical access controls

- Office Access controlled via secure entry control features
- Visitors are not left unattended with access to data or information
- No physical IT infrastructure / server
- Secure Physical Storage for hard copies of documents and mobile computing devices not otherwise secured by chain and lock.
- Clean desk policy

4.2 Archiving

All company records are maintained for a minimum period of seven years.

We are a digital first company and hard copies only retained where required.

Archiving arrangements for all client data is recorded, and considered in line with our Data Destruction Policies – see below.

4.3 Data Destruction

Data flows documentation is in place in respect of all data flows. This also records all locations where data is held, e.g. the data journey via email receipt, sFTP receipt, transformation, load. We then automate the destruction of all data that is not required to be held at any location to which it has been saved as part of the data journey.

See also the Funds-Axis Customer Data Policy.

5. Information Classification and Handling

5.1 Policy and Criteria

Company policy is to protect important or sensitive data and information held by the company by various means including access controls. This restricts access to only authorized personnel who have a justified and approved business need and those who require to use or have access to this information as part of their normal role within the company as a means of protecting the company against deliberate or unintentional loss of data or information. To assist in achieving this, the company uses the concept of Restricted Information.

5.2 Access and security requirements based on levels

Soft copies of Restricted Information are saved in restricted access folders in the Microsoft 365 Sharepoint Collaboration Portal.

These folders are

- Management Folder – senior management team only
- MD Folder – company Managing Director only
- Client Data Folder – Funds-Axis processing staff only

Within the Management folder all employee related data, information, copies of employment contracts, payroll details and the like are saved in the HR folder.

Access to these folders is restricted by the Microsoft 365 Sharepoint Collaboration Portal with access permissions controlled through the Access Control Matrix.

Hard copies of Restricted Information may only be held in the company's secure storage facilities (detailed at the Physical & Environmental Security section).

Access to Customer Data is restricted to only those Members of the Team providing Operational Support to Customers, with no access permitted to other functions including Technology Team, Finance, HR and other support functions.

5.3 Mobile Computing Devices

The company recognizes that mobile computing devices represent an increased risk of data / information loss through accidental loss or theft of the machine. Accordingly, all company laptops must have encryption security features as detailed in the Network Security section of this Policy.

5.4 Use of Non-Disclosure Agreements (NDAs) and Confidentiality clauses.

The company uses NDAs to protect Company restricted information when in discussions with suppliers, potential customers or other third parties. The Company's standard employment contract also includes confidentiality and Intellectual Property clauses to ensure staff clarity on responsibilities in the handling of certain key information.

5.5 Personal Data and Information

The Company does not hold personal data or information for the purposes of its business other than data and information on employees and used solely for company administration purposes.

We do not receive from clients any transfer agency data which includes any data in respect of individual unitholders.

5.6 Disclaimers

Appropriate disclaimers are included on all e-mail messages, the company's website, and the Information Portals.

5.7 Archiving and Destruction

5.7.1 IT Assets

The company operates a defined IT Asset Decommissioning and Disposal Procedure for all IT assets to ensure no data or information is lost accidentally when such assets reach the end of their useful lives. This is detailed at the Asset Management section.

5.7.2 Hard Copy Documents

We are a digital first company and hard copies only retained where required. Hard copy Restricted Information documents are held in secure storage on the company's premises. Documents which are no longer required are destroyed through the company's Classified Waste Disposal Facility.




5.7.3 Procedures / Controls

Restricted folder access controls – IT System Access Review and Change Procedure

IT Asset Acquisition, Decommissioning and Disposal Procedure

5.7.4 Labelling of Information – managing classified information

The following steps are undertaken to manage classified information:

1. Asset entered into Information Asset Inventory:
 - a. The asset Inventory is in the form of a Data Retention Table which indicates records, retention period, classification, and owner. This allows Funds-Axis to identify which classified information is in the company's possession and who is the owner.
2. Classification of information – following the risk assessment, each asset is classified on the basis of confidentiality:
 - a. Confidential (top confidentiality level) e.g. finance records, HR records
 - b. Restricted (medium confidentiality level) e.g. client information (Client data, reports, dashboards, compliance results, regulatory reports and any other Funds-Axis outputs relating to the client, client legal agreements, pricing, or tender correspondence etc.). This is defined as any client, company or employee data, documents, or information the loss of which could cause the Company financial or reputational damage or expose the company to legal action. Access to and storage of this data and information is consequently controlled more closely than non-restricted information. Company Restricted Information will include, but not be restricted to, company legal agreements, intellectual property, management accounts, statutory accounts, financial analyses, client listings, employee listings, strategic review documents etc. Employee Restricted Information will include, but not be restricted to, payroll records, personal details, employee listings, signed employment contracts, private employee correspondence, employee performance appraisals etc. To assist in identifying and managing restricted information the following sub-classification and controls are also used with the relevant classification in the document footer:
 -  Sensitive – for directors only. Requires password if sent by e-mail. Internal Use only
 -  Private & Confidential
 -  Client data – Private & Confidential and requires password if sent by e-mail
 - c. Internal use (lowest level of confidentiality) e.g. policies and procedures
 - d. Public (everyone can see the information) e.g. website, privacy notices

3. Information labelling:

- a. Information classified as confidential must be labelled 'Confidential' in the header/footer of each electronic file or in the top right-hand corner of hard copy HR folders.
- b. Information classified as restricted must be labelled in the following ways:
 - i. Email: email footer labels the information as strictly confidential
- c. Information classified as 'Internal' must be labelled in the following ways:
 - i. Electronic: using the 'Internal' template
 - ii. Label as 'Internal' in the header of the document
 - iii. Information classified as 'Public' will not be labelled

6. Human Resource Security

Overall HR Policy (A 1.2) is to put in place a framework of requirements, procedures and controls to ensure that:

- employees understand their responsibilities and are suitable for the roles for which they are considered
- employees are aware of and fulfill their information security responsibilities
- the company's interests are protected during the process of changing or terminating employment

6.1 Pre-Employment

Recruitment Policy (A 1.2.2)

The company operates a rigorous recruitment procedure. Role profiles, setting out the detailed requirements for the role, are in place for all new roles and the company operates a rigorous interview and selection process. The procedure seeks to ensure that successful candidates are those best qualified and fit for the role.

As part of the Joiner Procedure (A 1.2.3) extensive background checks are made, including references, identity and other checks, to verify the identity, qualifications and other information provided by the prospective employee. This is evidenced in the company Pre-employment Screening Checklist completed for each joiner.

A standard Contract of Employment and Staff Handbook (A 1.2.1) are provided to prospective employees. These set out clearly for the prospective employee their responsibilities in respect of Information Security.

6.2 Staff Handbook (A 1.2.1)

The Company's Staff Handbook reminds staff of their information security and data protection responsibilities, including in respect of:

- Information Security & Technology Controls Policy
- Password Protection Policy
- Clean Desk Policy
- Responsibilities for the security of the IT assets they use
- Email use
- Use of the internet
- Use of encryption
- Acceptable social media policy
- Prohibition on use of portable storage and media devices

Training on this is provided to new staff as part of the induction process. New staff are provided with a copy of the Staff Handbook when joining the company.

All staff then receive annual familiarization with the Handbook and provide an annual declaration that they have read and understood the employee responsibilities contained in the Handbook.

6.3 Training

Induction Training

Information Security training is included in employee Induction Training setting out the importance of this area and reinforcing employee responsibilities from the start of their employment.

Information Security Training

Information Security Awareness and Refresher Training is a mandatory for all employees. A module on this and familiarization with the Staff Handbook is provided through the Company's regular training sessions. There is also mandatory testing of this training.

Regular updates are provided on specific topics of information security training. Training records are held by the HR department.

Work from Home Training – see 2.2

Specific Information Security Qualifications

6.4 Annual Declaration

Each employee must complete an Annual Staff Declaration to reinforce awareness and the company's requirements relating to information security. In the Declaration staff must confirm, amongst other things, various matters in relation to information security, in particular that they have:

Completed their mandatory Information Security Training

Completed and passed the Annual Information Security Test (ATLAS Funds Training)

Read and understood the requirements detailed in the Company's Staff Handbook, including those relating to Information Security

6.5 Termination of Employment

The Company recognizes the higher risk associated with an employee leaving the company or having their employment terminated. The Company's Leaver Procedure ensures immediate removal of all employee system access upon leaving the company with audit evidence maintained on the BambooHR system.

6.6 Procedures / Controls

A 1.2.3 Joiner / Leaver Procedure

A 1.2.3.1 Pre-employment Screening Checklist

A 1.2.2 Recruitment Policy

A 1.2.1.1 Annual Staff Declaration (Staff Handbook etc.)

Mandatory Information Security Training & Testing

7. Asset Management

7.1 Asset Management Policy

The company's overall asset management policy is to maintain a framework of procedures and controls to ensure

- strict control over asset use for proper business purposes
- the physical security of assets (particularly mobile computing assets)
- appropriate hardware specification of assets and software load to maintain appropriate capacity and security features
- specific asset responsibilities clearly allocated to individuals to reinforce control

This framework seeks to mitigate the risks to the business of loss of assets or loss of information and maintain adequate capability and capacity to meet business processing and security needs on an ongoing basis.

7.2 IT Asset Register

An Inventory of all company physical IT assets is maintained in the Company Asset Register. This Register is maintained by the ISO who records all asset additions and disposals. All company IT assets have an identity marker on them with a unique reference number for identification purposes.

Company IT assets comprise all company PCs, laptops, mobile dongles, printers, and scanners.

7.3 Purchasing/acquisition and decommissioning / disposal of assets

The disposal of any device that can process or store data (PCs, laptops etc.) is done under a secure decommissioning and disposal process (A 1.7) to ensure that any company or client data has been wiped from the device prior to disposal.

Upon receipt computer devices are loaded with the Company's authorized list of software (including version / release).

7.4 Designated IT Asset Custodian

All IT assets have a designated custodian, which is recorded on the Asset Register. In most cases the custodian will be the individual who uses the asset on a day-to-day basis. For commonly used assets (e.g. printers) the custodian will be a named individual (e.g. ISO).

The custodian's responsibilities for assets are as follows –

- the day-to-day security and operation of the particular asset (for staff members, generally the IT asset they work with on a day-to-day basis)
- reporting any faults or operational performance issues with the asset to the ISO
- restricting physical access to the asset by securing it to the desk, locking it or closing it down when not in use
- observing the company's policy relating to the restrictions on the use of the machine (approved software only and no access to certain specified websites and types of website)

7.5 IT Equipment Maintenance

All IT equipment has anti-virus software and anti-malware software. Backups take place daily. Annual PAT testing takes place.

7.6 Stock take

A full stock take of the Company IT Asset estate is undertaken each year. For computer devices a check is also made that all software loaded on the machine conforms to the company's approved list of software (including version / release). Any unauthorized software is removed, and this is logged for appropriate follow-up with the asset custodian.

7.7 IT Asset Capacity and Software

The Register also records the processing and memory capacity of each PC / laptop. An Approved listing is maintained of all software (including version / release details) to be used in the company's network. This information is used for managing the company's computer asset estate.

A regular review of capacity issues is done by senior management to ensure all software and hardware assets remain fit-for-purpose given the developing needs of the business.

7.8 Role of ISO

The ISO has the following responsibilities in relation to IT Assets and the Asset Register

- \\ Maintaining the Asset Register: accuracy, completeness, up to date
- \\ Annual stock take and follow-up / escalation of discrepancies
- \\ Designated custodian (see definition below) for common use IT assets (printers, certain PCs and laptops)

7.9 Staff Responsibilities

All IT Assets have a designated custodian as recorded in the Asset Register. All staff members are likely to have custodian responsibility for at least one IT asset and their responsibilities are as detailed in the Designated IT Asset Custodian section above.

7.10 Procedures / Controls

- \\ IT Asset Stock takes – full annual stock take
- \\ IT Asset Register
- \\ A 1.7 IT Asset Acquisition, Decommissioning and Disposal Procedure
- \\ Hardware specification including security features for acquired assets
- \\ Asset custodian role

8. Access Control

8.1 Access Control Policy

The Company operates an access control policy and related procedures to ensure appropriate access rights, restrictions for specific user roles and access control rules for IT systems and information. This is designed to limit access to information and information processing facilities as appropriate to the user's role, the security requirements of business applications and the classification of information.

8.2 IT Access Control Matrix

Individual access is controlled at an overall level through the IT Access Control Matrix ("ACM"). This matrix sets out permitted user access rights for every company employee and any external system users and is reviewed and approved on a regular basis (at least every 6 months). The matrix is updated on an ongoing basis through the Joiner / Leaver process and as changing business requirements dictate (e.g. following a change of department by an employee), through the IT System Access Review and Change Procedure.

8.3 General Access Rights

The permitted general access rights for user groups for the different systems used by the company are restricted in line with individual roles and duties. General access to all systems is controlled via username (which must identify a specific individual) and password.

8.4 Privileged Access Rights

Privileged access rights comprise any rights over and above simple user rights and relates to System Administrators or other types of super-user. The granting of such rights to an individual must be in line with their role and duties and is subject to ISO approval.

8.5 Password Protection

Passwords must be used to protect access in line with the Password Protection Policy. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

8.6 Multi-factor authentication

To the greatest extent possible our policy is to only use third party applications that utilise MFA. This includes maintaining a register of all applications, whether they facilitate MFA, whether it is activated etc. For any applications not using MFA, these are risk assessed, including by whether they contain any customer data and whether access is restricted behind VPN etc.

For our own applications, all applications with customer data will be accessible only via MFA by end 2023.

8.7 User Registration and De-registration

Joiner / Leaver process

A key business risk is continued system access for users who have left the business. The company Leaver process ensures prompt and complete removal of system access for all company leavers.

IT System Access Review and Change Procedure

This Procedure covers ad hoc requests for system access changes when a user needs amended access rights in the normal course of business. This ensures effective control over such requests, particularly for new privileged access requests, and appropriate approval.

For all User Registration or De-Registration requests the ACM is update immediately by the ISO, subject to the necessary audit evidence being provided.

8.8 Procedures / Controls

IT System Access Review and Change Procedure.

IT System Access Control Matrix

Joiner / Leaver Procedures

Password Protection Policy

9. Physical & Environmental Security

The Company operates a variety of physical and environmental security procedures and controls with the overall objective of preventing:

- Unauthorized physical access, damage and interference to information and information processing facilities
- Loss, damage, theft or compromise of assets and interruption to operations
- Damage to assets through dust or soiling

9.1 Office Access

Funds-Axis operates from an office location in Belfast, Northern Ireland, with another office in Chennai in India. The physical controls in place include:

- Premises are secured when unoccupied with security guard present in the Business Park 24 hours a day, 7 days a week
- Restricted list of office key holders
- Office Access controlled via digital lock system with regular access code update
- Visitors are not left unattended with potential access to restricted information
- Secure storage for hard copy confidential or sensitive data and unsecured laptops in locked cabinets
- Staff observe a Clean Desk Policy.
- Confidential waste disposal facility

There is a close of business check every evening that all secure storage areas are locked, doors locked, and windows closed.

9.2 List of Key Holders

An approved list of keyholders is maintained for the office and secure storage areas within the office. These lists are reviewed regularly in conjunction with the ACM review procedure.

9.3 Secure Server Location and Access and Secure Storage

There is no physical server.

Mobile computers (e.g. laptops) are secured to desks by computer locks and chains or stored in secure locked cabinets.

Any physical company or client documents classified as Restricted Information are stored in secure locked cabinets. This includes client contracts, company legal documents, employee files and so on in line with the Information Classification and Handling Policy.

9.4 Cabling Security

Power and telecoms cabling carrying data or supporting information services is protected from interception, interference, or damage. All cables are protected from damage behind wall-mounted trunking. Ethernet CAT6 cabling is used as it has more stringent specifications for crosstalk and system noise.

9.5 Clean Desk Policy

A clean desk policy is observed ensuring no client or company sensitive paperwork is left unsecured overnight or when the office is closed. The policy is tested through unannounced checks by the ISO.

Further detail on how this operates, and staff responsibilities is included in the Clean Desk Policy document.

9.6 Confidential Waste Disposal

Any client or company sensitive paperwork to be disposed of is done so through the Confidential Waste Disposal Facility located in the office. The Confidential Waste facility is emptied, and the contents disposed of regularly in line with the requirements of a Confidential Waste Contract.

9.7 Record Storage

All hard copy company records are stored onsite. These are retained for a minimum period of seven years or agreed timeframe with client.

9.8 Procedures / Controls

Office Door Access System (Digital entry control)

Secure storage areas Visitor Procedures

Authorised List of Keyholders

Joiner / Leaver Procedure – Physical Access Changes

Clean Desk review

Confidential Waste Contract

Laptop Lock and Chains

10. Operations Security

Operations security procedures and controls are designed to ensure

- ✓ Correct and secure operation of information processing facilities
- ✓ Information and information processing facilities are protected against malware
- ✓ Appropriate back-up procedures are in place to protect against loss of data
- ✓ Event logs are kept and provide evidence for review and follow-up as required
- ✓ Installation of software is controlled to ensure ongoing integrity of operational systems

10.1 Documented Operating Procedures

The company maintains a comprehensive library of documented Operating Procedures in the Final Procedures folder with a reference document entitled FA Policies & Procedures List. This reference document and library are accessible to all staff.

Individual Operating Procedure documents are subject to regular review and update by a specified responsible person to ensure the document remains accurate, up-to-date and clear on the operation of the relevant procedure.

All Information security related policies and procedures are listed in the first page of this IS&TC Policy document and in staff training materials for reference.

10.2 Change Management Server:

We utilise Microsoft 365 Sharepoint Collaboration Portal instead of a server. Changes are limited to:

- ✓ Addition or removal of users
- ✓ Amendment to user permissions
- ✓ Addition or removal of folders
- ✓ Addition or deletion of new software on the network controlled via Microsoft Group Policy Settings

Change management is restricted in the following ways:

- Administration is via Administrator log-in only. Approval of Administrators is controlled via the Access Control Matrix and related procedures.
- Review of access levels and user changes is performed on the relevant server logs.
- Addition or deletion of new software on the server is controlled via Microsoft Group Policy Settings

Funds-Axis Software Change Request Management

Changes to the front end of the Funds-Axis Application are controlled through the Funds-Axis Change Request Management process.

New information systems, upgrades and new versions shall be tested before final sign-off and rollout by the company.

10.3 Capacity Management

The company actively monitors its network resources (including through the Office 365 Portal) to ensure these continue to perform to the level required.

These are reviewed on an ongoing basis by senior management and considered in conjunction with other information regarding system performance and technology developments to ensure the network and its key constituent parts have the capacity to continue to operate as required.

10.4 Protection from Malware

Webroot antivirus software is installed on the system to protect against various forms of malware. This is described in more detail in the Network Security section.

10.5 Server Back-up and Recovery

We utilise Microsoft 365 Sharepoint Collaboration Portal instead of a server. This includes back-up and recovery.

Nimbus are contracted to provide adequate resourcing and support to ensure that the Funds-Axis network can be fully restored with 24-hours.

Back-up and Recovery Testing

Testing of Back-up and Recovery Procedures is conducted regularly to check

- \\ Back-up procedures are working
- \\ Documents can be recovered within Business Continuity Plan timelines

The tests comprise a sample of folders or files both currently active and inactive chosen at random. Cyber Security are then requested to recover these items from the last back-ups (both local and cloud). These are compared to the a copy of the folder or file taken prior to the request going out to check that back-up procedures and recovery timeframes are operating as documented.

10.6 Logging and Monitoring

A server event log is automatically created and maintained by the server and is accessible through the Office 365 platform.

The server logs automatically a series of events which includes failed logins, exceptions and faults etc. but does not audit every single action taken or even events such as successful logins by default.

Logging facilities and log information are protected against tampering by logs being restricted to administrator access only.

10.7 Installation of Software on Client Operational Systems

There is only one client for which software is installed on Client Operational Systems. The software is packaged software and overall control of software on any company system or machine is controlled via Microsoft Group Policy Settings. Local Administration rights have been removed for individual users ensuring no ability to load unauthorized, or indeed, any software. The approved list of software on Group Policy is approved by the Managing Director.

10.8 Monitoring Activities

Funds-Axis is committed to monitoring networks and systems for anomalous behavior, having understood what 'normal' behavior/usage looks like. This is achieved through robust monitoring measures using Office 365, Microsoft Security Centre, Intune, and other tools.

Monitoring Measures:

Understanding Normal Behavior:

- \\ Continuous analysis of network and system behavior to identify deviations from the established baseline.

Anomaly Detection:

- \ Office 365 Monitoring: Utilizes Office 365's built-in monitoring tools to detect unusual activities, such as abnormal login attempts, data access patterns, and email usage.
- \ Microsoft Security Centre: Leverages Microsoft Security Centre to monitor security events, detect threats, and provide real-time alerts for anomalous behavior.
- \ Intune Monitoring: Uses Intune to monitor device compliance, configuration changes, and security status, ensuring that all devices adhere to company policies.

Incident Response:

- \ Automated Alerts: Automated alerts are generated for any detected anomalies, allowing for immediate investigation and response.
- \ Incident Reporting: A clear procedure for reporting and responding to potential security incidents is established. Employees are encouraged to report any suspicious activities or potential breaches.
- \ Investigation and Remediation: All reported incidents are promptly investigated, and appropriate remediation actions are taken to prevent recurrence.

Access Controls:

- \ Role-Based Access Control (RBAC): Access to monitoring tools and data is restricted based on user roles and responsibilities. Only authorized personnel can access and manage monitoring configurations.
- \ Multi-Factor Authentication (MFA): MFA is enforced for accessing systems that manage monitoring activities, adding an extra layer of security.

10.9 Procedures / Controls

Sharepoint Access Controls

Group Policy Settings

Back-up and Recovery Testing Procedures

11. Network Security and Device Management

Network security procedures and controls are designed to ensure the protection of information in the company's networks and its supporting information processing facilities.

11.1 Network Description

The network infrastructure currently comprises:

- \\ An external Microsoft Sharepoint Collaboration Portal located on Office 365.
- \\ Approximately 80 computers that connect via the internet and multi-factor authentication to Office 365
- \\ Internet which can be accessed by wifi or ethernet
- \\ A number of wifi / ethernet connected printers.

Whilst we use IP Telephony, this works on separate dedicated internet connections.

11.2 Microsoft Sharepoint Collaboration Portals

Funds-Axis operate two Office 365 Organisations.

- \\ The Funds-Axis Corporate Office365. Restrictions include:
 - Access to this is strictly limited to devices which are registered on our Microsoft InTune Device Management.
 - Access is also subject to multi-factor authentication.
 - There is also a restriction on the devices which can be so registered.
 - This is restricted to Funds-Axis Corporate devices, including Funds-Axis Corporate mobile phones and tables. This means that no personal devices including personal phones and tablets or laptops can be used to access our Office 365 email, sharepoints and Teams etc.
 - All users are required to be using a Funds-Axis email address. This includes any contractors, consultants.
 - Restrictions also prevent the sharing of any data / files with people outside of our organization; and
- \\ The Funds-Axis Collaboration Site – this is used for any sharing of data with third parties. This site is strictly controlled in terms of content and access rights. This data can also be accessed by mobile devices. The third parties do not need to have a Funds-Axis email address. This does

not require the third parties to use Funds-Axis devices or to use multi-factor authentication. The third parties do, however, need to be registered as Guests in our Organisation.

The above segregation enables easier control, risk assessment and oversight.

11.3 Device Management

Mobile computing devices (laptops, smartphones, tablets, convertible laptops, and various other personal computing devices) are important in today's computing environment. Their size, portability, and ever-increasing functionality are making the devices desirable in replacing traditional desktop devices. However, the portability offered by these devices can also increase security exposure to individuals using the devices.

Mobile Devices Generally

All mobile devices, whether owned by Funds-Axis or owned by staff, that have access to systems and applications are governed by this policy. Applications, including cloud storage software used by staff on their own personal devices are also subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

- \\ Mobile computing devices must be protected with a password required at the time the device is powered on
- \\ Passwords must meet the requirements outlined in the Funds-Axis Access Control and Password Policy
- \\ All data stored on mobile devices shall be encrypted
- \\ Wireless encrypted security and access protocols shall be used with all wireless network connections
- \\ Staff shall refrain from using unsecured network connections while using their mobile device for work
- \\ Personal mobile computing devices that require network connectivity must conform to all Funds-Axis standards for use and configuration
- \\ Personal devices should not be used for work business
- \\ Outside of our own dedicated secure offices or outside of the home,
 - Mobile devices should not be left unattended unless they are physically secured; and
 - Screen Privacy shields must be used.
- \\ Mobile computing devices that access the Funds-Axis network shall have active and up-to-date anti-malware and firewall protection
- \\ Lost and stolen devices shall have location services enabled and the units "bricked" or wiped of all information so they are unusable until recovered or destroyed

User responsibilities

The following procedures and requirements shall be followed by all users of mobile devices:

- \\ Staff shall immediately report any lost or stolen devices
- \\ Unauthorized access to a mobile device or company data must be immediately reported
- \\ Mobile devices shall not be “rooted” or have unauthorized software/firmware installed
- \\ Staff shall not load illegal content or pirated software onto any mobile device
- \\ Only approved applications are allowed on mobile devices that connect to the Funds-Axis network
- \\ Mobile devices and applications shall be kept up-to-date
- \\ Operating system and application patches should be installed within 30 days of release
- \\ Mobile devices shall have active and up-to-date anti-malware/virus protection software
- \\ All mobile device physical storage partitions shall be encrypted
- \\ Staff shall only use Funds-Axis corporate email system when sending or receiving Funds-Axis data
- \\ Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis
- \\ Mobile Device Management (MDM) will be used to enforce common security standards and configurations on devices
- \\ Staff shall not modify configurations without express written authorization from the ISO.

ISO Responsibilities

The ISO or their designee shall ensure:

- \\ Specific configuration settings shall be defined for personal firewall and malware protection software to ensure that this software is not alterable by users of mobile and/or employee-owned devices.
- \\ Annual security training is provided to users of mobile devices. The content and form of that training shall be decided by Funds-Axis or their designee. Periodic security reminders may be used to reinforce mobile device security procedures.
- \\ MDM software is used to manage risk, limit security issue, and reduce costs and business risks related to mobile devices. The software shall include the ability to inventory, monitor (e.g.

application installations), issue alerts (e.g. disabled passwords, categorize system software (operating systems, rooted devices), and issue various reports (e.g. installed applications, carriers).

- \\ MDM software enforces security features such as encryption, password, bricking, and key lock on mobile devices.
- \\ MDM software shall include the ability to distribute applications, data, and global configuration settings against groups and categories of devices.
- \\ Regular reviews and updates of security standards and strategies used with mobile computing devices.
- \\ Procedures and policies exist to manage requests for exemptions and deviations from this policy.

The ISO Team shall implement procedures and measures to strictly limit access to sensitive data moving to and from mobile computing devices since these devices generally pose a higher-risk for incidents than non-portable devices.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Funds-Axis IS&TC policies. Satisfactory examples of evidence and compliance include:

- \\ Spot user checks for compliance with mobile device computing policies
- \\ Readily available processes and procedures for staff use of mobile devices
- \\ Configuration and support guidelines and procedures for mobile devices
- \\ Communication and device logs of attached units showing appropriate management and monitoring protocols are in place
- \\ Anecdotal and archival communications showing regular implementation of the policy

11.4 Security Features

Security Measure – Technology	Provider & Details
Azure AD All devices are registered all devices on Azure AD InTune is part of the Microsoft 365 Licence Productivity Suite. This includes Office 365, Teams, OneDrive, SharePoint	The benefits of using Azure AD include: <ul style="list-style-type: none"> \ Single Sign-On, \ 2Factor Authentication, \ BitLocker on each device. \ advanced security features \ full back up of email \ EM+S \ Central management of all users via InTune \ Mobile device Management \ Remote wiping of desktop
Microsoft 365 Sharepoint Access restrictions	Roles and Permissions based access to Sharepoint sites
Multi-factor authentication	Mandatory Multi-factor authentication required for Microsoft 365 Access
Microsoft Azure Intune Policy Settings Microsoft Windows technology deploys settings automatically, allowing central control, consistency etc across the network	Microsoft Windows technology provides the following main security features: <ul style="list-style-type: none"> \ Approved software only: Either MSI software or from approved list of non-MSI software set up on Group Policy \ Deploy updates automatically (MSI software) \ Remove local Administrator permissions \ Helps automate process for joiner / leavers \ Restricted folder access control \ Central control over individual machines e.g. blocks USB, automatic lock if machine not in use etc
Machine encryption (Bitlocker) Bitlocker encrypts the individual machine hard drive thus preventing data being accessed following loss or theft of device or drive.	Microsoft Bitlocker <ul style="list-style-type: none"> \ Used on all laptops \ To be applied on all PCs as part of a rolling upgrade of the company's PC estate \ External local back-up drives are also encrypted using Bitlocker \ TPM 2.0 module
Password Manager (LastPass) LastPass stores and retrieves staff credentials in a secure manner.	Password Manager <ul style="list-style-type: none"> \ Requires Multi-Factor Authentication to access \ Long Passwords are randomly generated.

	<ul style="list-style-type: none"> \\ Credentials can be securely shared with Internal teams. \\ Security Assessment of user credentials
--	--

Security Measure – Technology	Provider & Details
EndPoint Protection End point protection for all machines, even when off network (and therefore outside the firewall)	Webroot End point protection provides the following: <ul style="list-style-type: none"> \\ Anti-virus, anti-malware \\ Storage Blocking (Mobile devices – USBs, mobile phones etc) \\ FTP Port Blocking \\ Data Loss Protection \\ Web Blocking
Anti-virus / Anti-malware Signature-based antivirus looks for and eradicates malware on the system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.	Webroot EndPoint Protection / Watchguard Firewall
DNS Filtering – web-blocking	Web blocking – URL filtering allows blocking of individual websites or by category, including storage <ul style="list-style-type: none"> \\ Blacklists: what to block \\ White Lists: what specific websites to allow (e.g. data download FTP / client portal addresses) \\ Black and white lists applied using Firewall rules
Data Loss Protection (DLP) on Web DLP aims to stop data moving out of network via web	MS Defender ATP
Data Loss Protection (DLP) on Email	Microsoft Office 365 E3 (for senior management)
FTP Port Blocking	MS Defender ATP
Storage Blocking Blocks use of USBs and other mobile storage devices	MS Defender ATP / Microsoft Group Policy Settings

Other Network Security Measures	Details
Use of Secure FTP as preferred method of client data file transfer	Secure FTP is the only method of client data file transfer where possible

E-Mail transfer of client data using password protected attachments	All client data sent by email must have the client data in attachments rather than body of email and attachments must be encrypted using password protection.
Segregation	Basic segregation between management level and team level information on server.

Third party Applications

As a policy, user access is based on a “least privileges required model and multi-factor”, with the implementation of VPN, IP restrictions or MFA where available.

User access and privileged access to the different systems and applications in line with user role and requirements.

11.5 Server Firewall

A server firewall is in place that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. The purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

The firewall provides an essential layer of security that, combined with other measures, prevent attackers from accessing servers in malicious ways.

11.6 Intrusion Protection / Intrusion Detection

One of the purposes of the firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

Watchguard includes intrusion detection and protection.

11.7 Anti-Virus Protection

Anti-virus software runs on the and on the PCs. It is automatically installed on a PC the first time that the PC registers on the network.

We use WEBROOT internet security which is maintained up to date for live threats. Scans and monitoring activity are as follows -

- Hourly security scans with a full weekly security scan preventing or detecting any threats, viruses or malware

- Monitoring reports produced daily and weekly showing the status of virus protection on the server and all machines and scanning frequency

11.8 Bitlocker / Machine Encryption

Bitlocker prevents data being accessed by theft of device or drive through encryption of the hard drive. The external local back-up drive is also encrypted with Bitlocker-to-go. All laptops handling client data are encrypted using TPM chip / Bitlocker.

Windows Bitlocker for units with a TPM chip do not need a key on start-up. The chip stores the encryption key. The login is the normal domain login in this instance, no other is needed to protect data.

11.9 FTP Access

The firewall by default blocks FTP ports 21 and 22 by the implicit deny rule. We therefore have to explicitly allow any FTP access for the purposes of transferring client data.

11.10 Computers: PCs and Laptops

Funds-Axis has a number of laptop and desktop computers. To support TPM encryption (see below), these need to be Windows 8.1 or newer. The basic standards for all new machines are Intel core I5, CPU @ at least 2.20 GHZ, Installed memory RAM 8 GB and TPM enabled.

We work on the assumptions that all machines may leave the office. This causes an issue as regards data loss in the event of the hard drive being damaged. It also causes an issue as regards data being at risk in the event of loss or theft of the computer.

To this end, there are a number of policies and controls in place, including:

- No company computer is accessible at all without a username and password. Access to Office365 is approved and controlled through the Company's IT Access Control matrix.
- Passwords are auto set up to require users to change them on a regular basis. These can also be changed by a system administrator logging in to Microsoft Office 365 portal.
- The use of Cloud based infrastructure means that anti-virus, DNS-filtering and other policies are automatically applied and kept up to date.
- All secure resources require access through the company VPN, with certs/keys protected by a passphrase and MFA.
- There are number of policies that are automatically forced down on to all machines, including:
- There is a policy in place preventing any data being saved onto the C:// drive. Data can be saved to OneDrive / Sharepoint. Accordingly, all data is saved on to the servers and subject to back-up.

- our policy is that all work documents should be saved to users OneDrives rather than to the computer hard drives.
- There is an enforced prohibition on the use of external media and data storage devices.
- We encrypt the hard drive using BitLocker Disk Encryption with TPM. TPM stands for “Trusted Platform Module”. It is a chip on your computer’s motherboard that helps enable tamper-resistant full-disk encryption without requiring extremely long passphrases.
- InTune provides us with the ability to remotely wipe all machines.

For business continuity purposes, we also have a stock of laptops permanently held offsite in order to support Business Continuity events.

11.11 USB / Mobile storage devices blocking

As a policy, there is disabling of the use of USB ports for remote hard-drives and for other devices that may have data storage capabilities including mobile phones and cameras. There is also Disabling of Bluetooth capabilities. This reflects the additional information security risks associated with mobile storage devices.

This is done via the Webroot End User Protection / Microsoft Group Policy.

11.12 Wi-Fi

The Company’s office premises has an internal Wi-Fi internet connection. This is password protected. This is wifi only and does not provide any access to servers etc. As above, there is no physical server.

11.13 Remote access

There is no physical server. All users access the Sharepoint Collaboration portal over the web. Remote access to computers is available to Nimbus Networks Limited who provide IT support. They can remotely access computers as needed to provide support. This is controlled through use of a named Administration account used by Nimbus only with access controlled by the company through password changes.

11.14 Website Blocking (including storage sites)

We utilise MS Defender ATP for website blocking, including by category that it is at endpoint.

We block access to a range of sites, including Storage Sites. This is done by

- Generally – Blocking by Category (Personal Blogs, Entertainment, Hosting)

2. Specifically - e.g. DropBox, Google Drive (just explicit sites).

A Blacklist and White List of sites is maintained showing websites blocked or explicitly allowed, respectively.

11.15 Web Filtering

Funds-Axis is committed to preventing users from accessing external websites that may contain malicious content or content that is not commensurate with organizational policies. This is achieved through robust web filtering measures using Defender XDR and Pi-Hole in combination with secure DNS with malicious address filtering.

Web Filtering Measures:

Defender XDR Web Filtering:

- \ Funds-Axis utilizes Defender XDR to block access to websites based on the following categories:
 - Blocked Categories:
 - Cults
 - Gambling
 - Nudity
 - Pornography/Sexually Explicit
 - Sex Education
 - Violence
 - Download Sites
 - Peer-to-Peer
 - Child Abuse Images
 - Criminal Activity
 - Hate & Intolerance
 - Illegal Drug
 - Illegal Software
 - School Cheating
 - Self-Harm
 - Weapons
 - Games
 - Instant Messaging
 - Social Networking
 - Web-based Email
 - Chat
 - Parked domains
 - Newly Registered Domains

Pi-Hole and Secure DNS Filtering:

In addition to Defender XDR, Funds-Axis applies blocklists on Pi-Hole in combination with secure DNS to filter out malicious addresses and prevent access to harmful websites.

Monitoring and Detection:

Continuous monitoring of web traffic to detect and block access to websites that fall under the blocked categories.

Automated alerts are generated for any attempts to access blocked websites, allowing for immediate investigation and response.

Access Controls:

Role-Based Access Control (RBAC) is enforced to ensure that only authorized personnel can modify web filtering settings.

Multi-Factor Authentication (MFA) is required for accessing systems that manage web filtering configurations.

Training and Awareness:

Regular training sessions are conducted to educate employees on the importance of web filtering and the risks associated with accessing malicious websites.

Awareness campaigns are run periodically to remind employees of the web filtering measures in place and their role in maintaining web security.

Incident Response:

A clear procedure for reporting and responding to incidents related to attempts to access blocked websites is established.

All reported incidents are promptly investigated, and appropriate remediation actions are taken to prevent recurrence.

11.16 Technical Vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the vulnerability evaluated, and appropriate measures taken to address the risk.

All Business Issues, with limited exceptions, are captured in ZOHO Bugs and Issues Tracker.

This captures all system bugs, issues and development requests.

All issues are classified, prioritised, and tracked.

Internal reporting is made in accordance with the agreed standards for Management and Board reporting having regard to issue classification and priority.

The above process includes identification of any technical vulnerabilities. For the avoidance of doubt, a weakness in respect of information security will typically be classified as Urgent, reported to Management and Board and there will be a related remedial action plan. This will include consideration of whether any additional disclosures are required to be made to Customers.

See Information Quality and Information Security Risk Registers.

11.17 Technology Control Monitoring reports

To ensure the on-going effectiveness of technology controls the following system generated reports are received and reviewed:

#	Report overview	Frequency	Received & reviewed by
1	Office 365 Reports	Monthly	Cyber
2	MS Defender ATP are available which show: <ul style="list-style-type: none"> the status of virus protection on all machines including date of last back-up; and any threats, viruses, malware prevented or detected by the security scans. 	Monthly	Cyber
3.	Intune and other reports to confirm: <ul style="list-style-type: none"> That bitlocker is installed on all machines That anti-virus is up to date The Microsoft updates are installed on all machines That sharepoint is being backed-up That right policies set on Office 365 DNS policies VPN installed and active 	Monthly	Cyber
4	Audit Reports and Back-up evidencing system user access reviews, including in respect of Sharepoint	Monthly	Cyber
5	Office 365 Health Reports, including on: <ul style="list-style-type: none"> In-bound and outbound messaging DLP 	Monthly	Cyber

11.18 Procedures / Controls

1. Asset Register and Audit Procedures

- Approved machines / devices on the network
- Physical audits to agree to Microsoft Sharepoint Logs and PC/Laptop specification including security chips and security software loaded (Bitlocker)

2. Microsoft Group Policy Settings –

- \ User access restrictions to certain folders

3. Review of Logs

- \ Devices accessing the network
- \ Check Group Policy Settings (software load)
- \ Approved Users
- \ User addition / deletion
- \ Network Support supplier access and usage log review

4. Machine Encryption (Bitlocker)

5. Physical and Logical Access Controls

- \ User Group Access: Folder Access restrictions
- \ Administrator Access and Review
- \ Restricted Folders Access (Group Policy Settings)
- \ Firewall Rules: URL filtering / Website Blocking categories,
- \ USB / Storage Devices blocked

6. Webroot Monitoring Reports

- \ Anti-virus status on all machines, intrusion / detection reports

7. Website blocking policy

- \ Approved Blacklist and White List
- \ Listing of Firewall Rules checked against approved Blacklists and White Lists.

12. Communications Security

Communications Procedures and Controls are designed to maintain the security of information transferred within the company and with any external party.

12.1 Client Data

The largest volume of data handled by the company relates to daily processes associated with the Funds-Axis Investment Compliance and Risk Monitoring products. The company operates a number of procedures to ensure the security and confidentiality of client data, including those set-out in this Policy and, more specifically, those set out in the separate **Policy Document: Funds-Axis Customer Data Policy**.

12.2 E-Mail

The company utilises Microsoft Office 365, including for email. Employees typically access this through the downloaded desktop application software or through their own personal mobile devices – phones and tablets. The use of webmail is not permitted.

12.3 Data Leakage Prevention

Funds-Axis is committed to preventing and detecting unauthorised access, transfer, or extraction of information through robust Data Leakage Prevention (DLP) measures. These measures are implemented to safeguard sensitive data, including client dashboards and company intellectual property (IP), such as code data.

DLP Measures:

Email Security:

- \ **Outlook DLP Configuration:** Funds-Axis utilises Outlook's DLP capabilities to prevent the unauthorised sending of client dashboards and sensitive information to external domains. This includes:
 - **Domain Restrictions:** Emails containing client dashboards are automatically blocked if sent to unauthorised domains.
 - **Content Inspection:** Emails are scanned for sensitive content, such as company IP and code data. If detected, the email is automatically blocked from being sent outside the company domain.

Monitoring and Detection:

- \ **Real-Time Monitoring:** Continuous monitoring of email traffic to detect any attempts to transfer sensitive information outside the company domain.
- \ **Alerting Mechanisms:** Automated alerts are generated for any detected data leakage attempts, allowing for immediate investigation and response.

Access Controls:

- \ **Role-Based Access Control (RBAC):** Access to sensitive information is restricted based on user roles and responsibilities. Only authorised personnel can access and handle sensitive data.
- \ **Multi-Factor Authentication (MFA):** MFA is enforced for accessing email accounts and systems containing sensitive information, adding an extra layer of security.

Training and Awareness:

- \ **Employee Training:** Regular training sessions are conducted to educate employees on the importance of data leakage prevention and the proper handling of sensitive information.
- \ **Awareness Campaigns:** Periodic awareness campaigns are run to remind employees of the DLP measures in place and their role in maintaining data security.

Incident Response:

- \ **Incident Reporting:** A clear procedure for reporting data leakage incidents is established. Employees are encouraged to report any suspicious activities or potential data breaches.
- \ **Investigation and Remediation:** All reported incidents are promptly investigated, and appropriate remediation actions are taken to prevent recurrence.

Anti-Virus

Office 365 provides robust email protection against spam, viruses, and malware with [Exchange Online Protection](#). Office 365 also offers [Advanced Threat Protection](#) (ATP), an email filtering service that provides additional protection against specific types of advanced threats.

Archiving and back-up

Office 365 does not back up your email. It offers native data protection, which includes multiple passive copies (lagged copies) split between two data centres. That provides for availability of existing data. This does not ensure a point-in-time recovery of data deleted that has gone past the deleted item retention period. The retention period is 14 days by default and can be extended to 30 days through a remote PowerShell connection.

Risk of data theft – Mobile device management

Office 365 offers mobile device management (MDM) as part of the subscription. This enables us to enforce policies such as PIN locking (or more complex passwords), sign-in failure counts, inactivity locks, device encryption, and preventing "rooted" or "jailbroken" devices from connecting.

Secure Email Transmission

Transport Layer Security (TLS) is a cryptographic protocol that secures communication over a network by using security certificates to encrypt a connection between computers.

We have configured “opportunistic TLS”. This means that Exchange Online always attempts to use TLS first to secure your email but cannot always do this if the other party does not offer TLS security.

When you send mail to a recipient within our organization, that email is automatically sent over a connection that is encrypted using TLS. Also, all email that you send to other Office 365 customers is sent over connections that are encrypted using TLS and are secured using Forward Secrecy.

However, the message will be sent unencrypted if the recipient organization doesn’t support TLS encryption.

We do have the option to enforce TLS.

Data and disaster recovery

Access to Outlook 365 is available over any web-connection through any device from anywhere in the world. Accordingly, it is subject to minimal business continuity risks other than total internet failure.

12.3 Procedures / Controls

A.1.13 Communications Security Procedure

13. Supplier Relationships

The Company's key IT suppliers are:

1. Amazon AWS
2. Fundsaxis India Private Limited – HighWire
3. Sisense

Supplier relationships are covered by contracts and service level agreements with regular review by management of operational performance as follows:

- ✓ SLA arrangements clearly define the responsibilities of AWS
- ✓ On-going monitoring and tracking of all system and service issues, to enable on-going evaluation of Miles
- ✓ At least bi-annual visit to offices, including to Fundsaxis India Private Limited in India
- ✓ Receipt and review of BCP plan and corporate documentation
- ✓ Obtaining and reviewing financials
- ✓ Regular service level meetings

13.1 Amazon AWS

Amazon AWS is our Technology hosting provider, including for the Highwire product, the integrated Sisense Reporting product and the Knowledge Portals. For further details of our relationship see the contractual Annexure on Cloud Computing.

13.2 Fundsaxis India Private Limited

Fundsaxis India Private Limited provide the HighWire technology that we make available to customers.

Our exposure to Miles is limited by the fact that the product is entirely managed and hosted by us on our Amazon AWS hosting to which Miles have no access and Miles cannot make any code releases.

In this regard, we take the following steps:

- ✓ Close relationship with Miles Software
- ✓ SLA arrangements clearly define the responsibilities of Miles Software

- \\ On-going monitoring and tracking of all system and hosting issues, to enable on-going evaluation of Miles
- \\ At least bi-annual visit to Miles offices in Mumbai
- \\ Receipt and review of Miles BCP plan and corporate documentation
- \\ Obtaining and reviewing Miles' financials
- \\ Regular service level meetings

Where any additional support is required from Miles Software, then that is provided subject to the following arrangements:

- \\ They will not make changes to the rules configuration module
- \\ They will not provide any third-party access
- \\ They will not access/download client data
- \\ They will not make any rule changes
- \\ They will not release code changes without Funds-Axis' permission, after proper testing in accordance with release management framework.

13.3 Sisense

Sisense provide the Business intelligence software that is integrated within our HighWire application.

Our exposure to Sisense is limited by the fact that the product is entirely managed and hosted by us on our Amazon AWS hosting to which Sisense have no access and Sisense cannot make any code releases.

13.4 Nimbus Networks

Nimbus Networks are contracted to provide adequate resourcing and support to ensure that the Funds-Axis network can be fully restored with 24-hours.

13.5 Big Wet Fish

The following information websites are maintained on a content management portal maintained by Big Wet Fish:

- www.Global Disclosures.com

- www.Global Exchanges.com

- Atlas

The information is captured and maintained on a content management portal made available by Big Wet Fish.

The main risks of a BCP event could arise in respect of any of the following components:

- The content – the content becomes incorrect

- The CMS package – the package is corrupted or the provider makes it unavailable

- The hosting service that the CMS and content sit on and which makes them accessible becomes unavailable.

13.6 The Hosting Service

As above:

1.1.1. Our Highwire and FundWare technology is deployed on the Amazon AWS cloud infrastructure.

1.1.2. Hosting is arranged by the CMS provider – Big Wet Fish. Our Portals are currently on low-cost, high-quality, single-location hosting solution.

14. Information Security Incident Management

All Incidents (as defined in the Incident Management Policy) must be reported to Senior management and recorded in the company's Incident Management System (IMS - ZOHO). Follow up, impact assessment and resolution of the incident will then be dealt with in line with the company's Incident Management Procedures.

This is designed to ensure that all such Incidents, including Information Security related Incidents, are reported, escalated and managed to ensure proper senior management control and visibility. This will in turn ensure that all information security implications are understood and addressed.

14.1 Information Security Incidents

An Incident is likely to have the following potential consequences:

- \\ may affect the uninterrupted flow of company operations
- \\ may cause financial or reputational damage to the company, or
- \\ may result in legal action against the company.

Examples of Information Security related Incidents include:

- \\ Theft or loss of a company laptop
- \\ Client data e-mailed outside the company without password protection
- \\ Finding restricted information, such as an employee HR file, sitting unattended on a desk
- \\ Client data or information disposed of in a normal waste bin (rather than Confidential Waste)
- \\ Unauthorised access to the IT network
- \\ Incidence of a computer virus on the company network
- \\ Company system outages or interruptions affecting the company or clients operations
- \\ Erroneous transfer of one client's data to another client

14.2 Procedures / Controls

Review of IMS Incident Logs and reporting to Board

15. Business Continuity and System Availability

The Company Business Continuity & Disaster Recovery Plan (BCP) has been designed to ensure that information security continuity is embedded in the plan and to ensure the availability of information processing facilities is maintained.

The key features of the BCP which ensure this are:

- \\ Detailed plans and procedures covering key potential business continuity events, related company responses and timeframes (reproduced below for reference)
- \\ Business impact analysis for each of the teams / functions within the company and their related Recovery Time Objectives (RTOs) and required resources, including IT resources, to achieve the RTO
- \\ Layered programme of regular IT back-up procedures to support any required IT recovery process
- \\ Programme of back-up checks and testing to maintain readiness for a Business Continuity event (See below)
- \\ Clear Roles and Responsibilities set out for specified individuals in the BCP with appropriate training to support ongoing readiness
- \\ Reliance on key IT suppliers identified and procedures for managing their potential business continuity event risk set out

15.1 Key Business Continuity Events

The specific technology reliance for certain key business continuity events, related actions and timeframes are summarised below:

#	Issue	Contact	Contingency	Time for Contingency Actions to take effect
3	Internet is not available \\ Telecomms failure or malfunction	BT	4G Wi-Fi Hotspots to be used in addition to BT Wi-Fi Public Wi-Fi not to be used	1 hour
4	Office Premises are not accessible / usable \\ Power Failure \\ Fire \\ Civil Disturbance	Nimbus Networks Regus	Directors Home / home remote working, via secure VPN / alternative Weavers Court offices Arrange short term Regus office etc. if longer requirement.	1-2 hours 2 days

5	Documents are lost – critical documents or in large numbers <ul style="list-style-type: none"> User error, malicious actions 	Nimbus Networks	This would require a restore of collaboration portal based on backed-up data.	6-7 hours
6	Computers are lost / damaged <ul style="list-style-type: none"> Small scale loss / damage event 	Dell / Other Supplier	Use contingency machines pending purchase of new computers	1-2 hours
7	Telephony is down <ul style="list-style-type: none"> Telecomms failure or malfunction 	BT	Use mobiles	Immediate

15.2 Training & testing Programme

Training:	<ul style="list-style-type: none"> Induction for new staff includes Business Continuity Plan awareness. Programme of briefings to ensure all staff are updated on BCP awareness on an annual basis. All staff who are named within this plan as having authority to invoke the plan or to be part of the Incident Response Team have been trained/ briefed on their role and responsibilities.
Testing:	<p>The following elements are tested routinely within the company's BCP testing process:</p> <ul style="list-style-type: none"> That all data is being properly saved on to collaboration portal That all collaboration portal data is being properly backed-up Alternative office and home working recovery capabilities are evidenced; Restoration of data within BCP timeframes An annual key IT Supplier Review is also performed BCP Contact Details maintained up-to-date

Details of the key BCP tests are as follows:

1. Data properly backed up

On a six-monthly basis a sample of test documents / files are created and then deleted. The sample of documents / files is chosen to ensure a spread of currently active and inactive items across different folders and areas of the business. It is then tested that these files can be recovered. Recovered documents / files are then compared to the original snapshot copies and findings recorded. Any discrepancies between the actual findings and documented back-up timings for different back-up systems are investigated.

2. Alternative office and home working arrangements

On an annual basis a portion of the Funds-Axis Team (covering 25% or more of clients requiring processes for that day) will operate from alternative premises. The alternative premises will be for the sole use of the company and have Wi-Fi connection. Full details of the test are recorded for audit purposes including clients / processes covered, location used, how contingency computers operated and whether SLAs were met.

3. Telecoms failure: Internet temporarily unavailable

On a six-monthly basis the company's Wi-Fi dongles are tested to ensure effective operation. This is done by switching off the internet connection to identified machines for a period (to cover a single clients full processes for that day) and putting them onto the dongle mobile connection. Full details of the test are recorded for audit purposes including clients / processes covered, upload / download speeds, and whether SLAs were met.

For further details of Continuity plans refer to the BCP document.

15.3 Procedures / Controls

- \ Periodic tests of recovery of specific documents / files from the different back-up systems ensuring recovery within specified BCP guidelines
- \ Periodic tests of home working / alternative office working for Funds-Axis team to ensure critical daily processes are completed within SLA
- \ Regular review and operation of contingency machines to ensure continuing fitness for purpose in a continuity event
- \ Staff training and communications

16. Contact with Regulatory Authorities and Special Interested Groups

Contact with regulatory authorities and special interested groups shall be maintained by the ISO. This shall include, but not be limited to:

- Information Commissioner's Office (ICO) – see A1.3 Data Protection Policy and A1.3.1 Data Breach Response Policy
- Key suppliers – see Business Continuity Plan Appendix for contact details

See also Context and Scope, section 2.3 Interested Parties Register.

17. Information Security in Project Management

Funds-Axis are required to include information security objectives in project objectives, perform a risk assessment in the early stage of the project, carry out treatment of the identified risks and implement security measures

Project Managers shall make the Information Security policy an indispensable part of all stages of the project.

17.1 System Development Life Cycle

The ISO shall establish and protect secure development environments for system development by implementing the following processes:

- Planning: thinking about and organizing all activities required to develop the system
- Analysis: gaining a better understanding of what is expected from the system
- Design: defining the solution to be implemented
- Implementation: executing the activities required to create the system and make it available to users
- Operation: the effective use of the system
- Maintenance: making changes to the system to ensure it does not become obsolete
- Disposition: discarding the system.

17.2 Change Management

The ISO is responsible for considering the impact on information security when changes to the following are planned or take place: changes to the company, business processes, information processing facilities and systems.

18. Compliance and Information Security Monitoring & Review

The company operates a comprehensive Risk Management Framework to ensure the following with regards to information security:

- \\ To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements
- \\ To ensure that information security is implemented and operated in accordance with company policies and procedures

18.1 Quality and Information Security Risk Registers

The Company's Risk Management Framework is structured as follows:

Procedures and Controls

- \\ Each IS&TC Policy section has specified Procedures and Controls designed to address the key risks identified in that area
- \\ Risks are identified in the Quality and Information Security Risk Registers

Control Testing and Audit Programme

- \\ The Control Testing and Audit Programme sets out the key audit tests to ensure overall effective Information Security controls operation
- \\ The performance of the underlying procedures and controls is operationalized through a rolling Monthly Controls Completion Programme providing evidence that the key procedures and controls have been completed.

Staff Awareness, Training and Testing

- \\ The company has a mandatory Information Security and Technology Controls Training module covering all aspects of this topic as it affects individual staff members
- \\ There is a mandatory online pass / fail test of the training session to reinforce staff learning and awareness of the subject
- \\ There will be ad hoc communications to staff as required for update or awareness on particular information security issues or incidents

18.2 External Accreditation

Funds-Axis are committed to retaining ISO 27001 certification.

Legal Requirements

The Company is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation is devolved to employees and agents of the Company, who may be held personally accountable for any breaches of information security for which they may be held responsible. Legal requirements and developments are reviewed on an ongoing basis by senior management and the Board.

The Company shall comply with the following legislation and other legislation as appropriate:

- \\ The Data Protection Act (1998) (until 24 May 2018) / General Data Protection Regulations 2018 (from 25 May 2018)
- \\ The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- \\ The Copyright, Designs and Patents Act (1988)
- \\ The Computer Misuse Act (1990)
- \\ The Health and Safety at Work Order (Northern Ireland) (1978)
- \\ Human Rights Act (1998)
- \\ Regulation of Investigatory Powers Act 2000
- \\ Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000
- \\ The Telecommunications (Data Protection & Privacy, Direct Marketing) Regulations 1999
- \\ Business Continuity Practice Guide: 2006 (UK Tripartite Authorities: Financial Services Authority (FSA), HM Treasury, Bank of England)
- \\ Companies Act 2006

18.3 Intellectual Property Rights

The company acknowledges that the intellectual property rights of proprietary software resides with the software's publisher and no counterfeit software is to be used. Only software to which the company has signed up to a license agreement is installed and used on company equipment. Employees and those working on the company's behalf are not permitted to download or install any software without express permission. Source code is not to be modified and software is not to be re-distributed.