

March 2025

INTERNAL

# AI Policy

FUNDS  AXIS

<b>Policy title:</b>	AI Policy
----------------------	-----------

<b>Issue</b>	1.0
<b>Approved by:</b>	Trevor Dempster
<b>Approval Date:</b>	March 2025
<b>Next Review Date:</b>	March 2026

<b>Scope:</b>	This policy applies to all employees, contractors, and third-party service providers who access the internet through the organisation's network and systems.
<b>Associated documentation:</b>	<ul style="list-style-type: none"> <li>\ A 1 Information Security Policy</li> <li>\ A 1.1 Risk Assessment and Risk Treatment Procedure</li> <li>\ Approved Software List</li> <li>\ A 9.5.1 Approved Suppliers List</li> <li>\ A 1.3 Data Protection Policy</li> <li>\ A.1.14.2.4 Change Management Process</li> </ul>
<b>Responsibility for Implementation &amp; Training:</b>	<p>Day to day responsibility for implementation: ISO</p> <p>Day to day responsibility for training: ISO</p>

<b>Distribution methods:</b>	<p>Methods used to communicate this policy:</p> <ul style="list-style-type: none"> <li>\ Training</li> </ul>
------------------------------	--

## 1. Policy Synopsis

At Funds-Axis, we recognise the rapid pace of change in artificial intelligence and automation technologies, particularly as vendors embed both proprietary and third-party AI into their products and services.

Our AI Policy reflects the following key principles:

1. **Third-Party AI Integration:** We expect that many third-party suppliers will integrate AI, both proprietary and third-party, within their tools.
2. **Supplier Oversight:** All suppliers are tracked in our Supplier Register, including information on whether client data is accessible to those vendors.
3. **Strict Access Controls:** No third-party tool is permitted unless explicitly approved by internal governance processes.
4. **Data Access by Vendors:** No supplier is allowed access to client data unless permitted in writing by the client and governed by a formal agreement.
5. **Risk-Based Review:** Regardless of client data access, all AI-capable tools are assessed for risk, reliability, data flows, and governance.
6. **AI Library Governance:** We maintain a controlled inventory of AI libraries (e.g. Python, AWS tools) to ensure each is secure, approved, and kept current.
7. **Controlled Innovation:** Team-led innovation is encouraged, but all solutions, especially those involving AI or automation, must follow defined SOPs and be implemented at a corporate level. No “DIY” automation, including Copilot usage, is permitted without central approval.

## 2. Purpose

This policy outlines the standards and controls governing the adoption, development, use, and procurement of AI systems at Funds-Axis. It ensures alignment with:

- ✓ **ISO/IEC 27001:2022** – particularly Annex A controls A.5 (Policies), A.7 (Human Resources), A.14 (System Acquisition & Development), A.15 (Supplier Relationships).
- ✓ **ISO 9001:2015** – especially around clause 8 (Operation) and clause 6 (Planning) for managing risk and operational excellence.

The objectives of this policy are:

- \\ To mitigate risks posed by AI technologies
- \\ To ensure secure and ethical use of AI.
- \\ To prevent unapproved access to sensitive or client data.
- \\ To support quality and consistency across business processes.

## 3. Scope

This policy applies to:

- \\ All Funds-Axis employees and contractors.
- \\ All systems, services, or processes involving AI or automation.
- \\ All third-party software, APIs, or platforms containing embedded AI.
- \\ All internally developed or deployed AI tools (including Microsoft Copilot).

## 4. Governance Framework

### 4.1 Corporate Control & Innovation

- \\ Innovation is welcome but must be centrally managed. All AI or automation-led enhancements must be:
  - Proposed via formal change request.
  - Reviewed for operational, information security, and legal risks.
  - Approved through the Corporate Library process.
- \\ Individual staff may not deploy or design their own AI processes, including Copilot actions, automation scripts, or new workflows, outside of approved SOPs.

### 4.2 Use of Digital Assistants

- \\ All digital assistants (e.g. local LLMs, internal chatbots):
  - Are deployed inside Funds-Axis' secure cloud architecture.
  - Are not connected to the internet or external services.
  - Cannot connect to HighWire or other production databases.
  - Must not export or transmit data externally.
- \\ Demo-specific exceptions require:
  - Documented client consent.
  - Temporary and controlled deployment.
  - Internal security approval.

## 5. Third-Party AI Governance

### 5.1 Supplier Approval and Risk Management

- \\ All third-party vendors are recorded in the A 9.5.1 Approved Suppliers List, including details of:
  - AI use in their platform.

- Client data access capability.
- Hosting model, including sub-processors.
- \ Use of any supplier software that contains AI must be approved through the Supplier Management process.

## 5.2 Access to Client Data

- \ No supplier is permitted to access client data unless:
  - The client has granted explicit written consent.
  - The access is contractually documented (e.g. in DPAs or contracts).
- \ This applies regardless of how “minor” or “background” the AI functionality may seem.

## 6. AI Libraries and Technical Tooling

- \ AI and machine learning tools sourced from platforms such as AWS Marketplace, Hugging Face, or PyPI must:
  - Be logged in the **Approved Software List** and/ or **Approved Supplier List**.
  - Be security-tested and reviewed.
  - Be subject to version control and lifecycle management.
  - Be removed if deprecated, end-of-life, or found to be insecure.
- \ The frequency of review will increase as dependency and tooling pace increases.

## 7. Client Meeting Recordings and AI Transcription

- \ As AI transcription and meeting summarisation becomes more common, Funds-Axis applies the following rules:
  - **Do not approve** client use of AI transcription (e.g. Fathom, Otter.ai) by default.
  - Respond politely declining such requests unless pre-agreed in writing.
  - Exceptions for demo environments may be permitted with:
    - Advance client approval.
    - A clear business reason.
    - Internal authorisation.
- \ Rationale: Transcripts create records which must be audited for completeness and security. Permanent storage by third parties is discouraged.

## 8. Compliance Monitoring

- \ AI usage is monitored and audited under the ISMS and QMS audit programs.
- \ Violations of this policy are treated as security incidents and may trigger disciplinary action.
- \ All staff must complete annual training on AI usage and risks.

- Internal audits will include AI usage and tool governance as a defined review scope from 2025 onward.

## 9. Policy Review and Change Management

- This policy will be reviewed annually or:
  - Following major regulatory changes (e.g. DORA, NIS2).
  - In the event of significant internal process or system change.
  - After major incidents or lessons learned.
- Changes are communicated through internal governance and included in staff re-training modules.