

May 2026

INTERNAL

# AI Policy

FUNDS  AXIS

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

<b>Issue</b>	2.0
<b>Approved by:</b>	Trevor Dempster
<b>Approval Date:</b>	May 2026
<b>Next Review Date:</b>	May 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

Funds-Axis recognises the rapid evolution of artificial intelligence and the increasing embedding of AI capabilities within enterprise software. This policy establishes strict governance over all AI usage to ensure compliance with ISO 27001, ISO 9001, client contractual obligations, and internal security standards.

Key principles:

1. **Embedded AI Awareness** - Many enterprise tools (including Microsoft 365) now include AI by default. These capabilities must be governed, restricted, and monitored.
2. **Supplier Oversight** - All suppliers are recorded in the Supplier Register, including whether AI is embedded and whether client data is accessible.
3. **Strict Access Controls** - No AI-enabled tool may be used unless explicitly approved through internal governance.
4. **Client Data Protection** - No supplier or AI system may access client data unless contractually authorised and approved in writing by the client.
5. **Risk-Based Review** - All AI-capable tools undergo risk assessment covering data flows, reliability, security, and governance.
6. **AI Library Governance** - All AI libraries and technical tooling are centrally controlled, version-managed, and security-reviewed.
7. **Controlled Innovation** - Innovation is encouraged, but all AI usage - including Microsoft Copilot - must follow approved SOPs. No personal or “DIY” automation is permitted.

## 2. Purpose

This policy ensures that all AI usage at Funds-Axis:

- ✓ Protects client and internal data.
- ✓ Complies with ISO/IEC 27001:2022 Annex A controls (A.5, A.7, A.14, A.15).
- ✓ Supports ISO 9001:2015 requirements for operational consistency and risk management.
- ✓ Prevents unauthorised or unsafe use of AI systems.
- ✓ Ensures transparency, auditability, and accountability.

## 3. Scope

This policy applies to:

- \\ All employees, contractors, and temporary staff.
- \\ All AI-enabled systems, including Microsoft Copilot for Microsoft 365.
- \\ All third-party AI tools, APIs, or embedded AI features.
- \\ All internally developed AI systems, including prototypes and proof-of-concepts.
- \\ All automation, scripting, or workflow tools that use AI or machine learning.

## 4. Governance Framework

### 4.1 Corporate Control & Innovation

All AI-related initiatives must:

- \\ Be submitted via formal change request.
- \\ Undergo information security, operational, and legal review.
- \\ Be approved through the Corporate Library and ISMS governance processes.

**Staff are prohibited from:**

- \\ Creating personal AI workflows.
- \\ Using Copilot to automate tasks without approval.
- \\ Deploying scripts, agents, or automations outside approved SOPs.
- \\ Connecting AI tools to production systems or client data.

### 4.2 Use of Microsoft Copilot for Microsoft 365

Microsoft Copilot is deployed on corporate devices but is **not approved for unrestricted use**.

Permitted use:

- \\ Internal productivity tasks (drafting internal documents, summarising internal emails, etc.).
- \\ Work involving **non-client, non-confidential** information.
- \\ Activities explicitly approved by management.

Prohibited use:

- \\ Entering client data, financial data, or regulated data.
- \\ Using Copilot to analyse or process client deliverables.
- \\ Using Copilot to generate code, scripts, or automation without approval.

Copilot usage is monitored and logged by Microsoft 365 audit tools.

## 4.3 CEO-Led Copilot Studio Working Group

A dedicated working group, reporting to the CEO, is responsible for:

- \ Exploring the development of internal AI agents using **Copilot Studio**.
- \ Ensuring all agents operate only on **non-client data**.
- \ Designing secure, auditable workflows aligned with ISO 27001 and ISO 9001.
- \ Producing governance documentation, SOPs, and risk assessments for any future deployment.

No Copilot Studio agent may be deployed without formal approval.

## 4.4 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. Prohibited AI Systems

To protect client data, intellectual property, and regulatory compliance, the following AI systems are **strictly prohibited**:

- \ **OpenAI ChatGPT (all versions)**
- \ **Anthropic Claude**
- \ **Google Gemini**
- \ **Perplexity AI**
- \ **Meta Llama-based public chatbots**
- \ **Amazon Q (public version)**
- \ **Any consumer AI app or website not explicitly approved**

**Use of these systems for any work-related activity is forbidden**, including:

- \ Drafting client communications
- \ Analysing data
- \ Uploading documents
- \ Generating code
- \ Brainstorming client-related content

## 5.1 Disciplinary Consequences

Unauthorised use of prohibited AI systems constitutes a security breach.

Consequences may include:

- \\ Formal HR disciplinary action.
- \\ Revocation of system access.
- \\ Mandatory retraining.
- \\ **Dismissal for gross misconduct** where client data or confidential information is exposed.

This aligns with ISO 27001 A.7 (Human Resources Security) and A.5 (Policies).

## 6. Third-Party AI Governance

### 6.1 Supplier Approval and Risk Management

All AI-enabled suppliers must be:

- \\ Logged in the Approved Supplier List (A.9.5.1).
- \\ Assessed for AI usage, data flows, hosting, and sub-processors.
- \\ Approved through Supplier Management.

### 6.2 Access to Client Data

No supplier may access client data without:

- \\ Explicit written client consent.
- \\ Contractual documentation (DPA, contract clause, or amendment).

This applies regardless of how “minor” the AI functionality may appear.

## 7. AI Libraries and Technical Tooling

All AI libraries (Python, AWS, Hugging Face, etc.) must:

- \\ Be approved and recorded.
- \\ Undergo security testing.
- \\ Be version-controlled.
- \\ Be removed if insecure, deprecated, or end-of-life.

The frequency of review increases with dependency and tooling pace.

## 8. Client Meeting Recordings and AI Transcription

Funds-Axis does **not** approve the use of third-party AI transcription tools (e.g., Otter.ai, Fathom) unless:

- \ Pre-approved in writing by the client.
- \ Approved internally.
- \ Used only in demo environments.

Transcripts are treated as records and must be securely stored and auditable.

## 8. Compliance Monitoring

- \ AI usage is monitored through ISMS and QMS audits.
- \ Copilot usage is logged through Microsoft 365 audit tools.
- \ Violations are treated as security incidents.
- \ Annual mandatory AI training is required for all staff.
- \ AI governance will be a defined audit scope from 2026 onward

## 9. Policy Review and Change Management

This policy will be reviewed:

- \ Annually.
- \ After major regulatory changes (e.g., DORA, NIS2, EU AI Act).
- \ After major incidents or lessons learned.
- \ When new AI capabilities are introduced into the Microsoft ecosystem.

Changes will be communicated through internal governance and included in staff re-training modules.