

February 2025

INTERNAL

# Threat Intelligence Policy

FUNDS  AXIS

<b>Policy title:</b>	Threat Intelligence Policy
----------------------	----------------------------

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

<b>Scope:</b>	This policy applies to all employees, contractors, and third-party service providers involved in the management and operation of Funds-Axis's information systems.
<b>Associated documentation:</b>	<ul style="list-style-type: none"> <li>All policies and procedures</li> </ul>
<b>Responsibility for Implementation &amp; Training:</b>	Day to day responsibility for implementation: ISO  Day to day responsibility for training: ISO

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

## Purpose

The purpose of this policy is to establish a framework for the collection, analysis, and dissemination of threat intelligence to enhance Funds-Axis's security posture and protect its assets from cyber threats.

## Scope

This policy applies to all employees, contractors, and third-party service providers involved in the management and operation of Funds-Axis's information systems.

## Definitions

- \\ **Threat Intelligence:** Information that has been collected, processed, and analysed to understand a threat actor's motives, targets, and attack behaviours.
- \\ **Indicators of Compromise (IoCs):** Artifacts observed on a network or in an operating system that indicate a potential intrusion.

## Policy Statements

- \\ **Collection:** The organisation shall collect threat intelligence from various sources, including threat intelligence feeds, security forums, industry reports, and government advisories. Specific sources include VirusTotal, AbuseIPDB, AlienVault OTX, and Microsoft Threat Intelligence feed.
- \\ **Analysis:** Collected threat intelligence shall be analysed to determine its relevance, accuracy, and potential impact on the organisation. Ingested data will be used by rules in the SIEM and MDR for improved insights and to block malicious sources.
- \\ **Dissemination:** Relevant threat intelligence shall be disseminated to appropriate stakeholders in a timely manner to ensure informed decision-making.
- \\ **Integration:** Threat intelligence shall be integrated into the organisation's risk management and incident response processes, with the Head of Assurance and Operational Risk meeting weekly with Heads of Departments to report to the board monthly.
- \\ **Review and Update:** The threat intelligence process shall be reviewed and updated regularly to ensure its effectiveness and alignment with the organisation's security objectives.

## Roles and Responsibilities

- \\ **Threat Intelligence Team:** Responsible for the collection, analysis, and dissemination of threat intelligence.
- \\ **Security Operations Center (SOC):** Utilises threat intelligence to monitor and respond to security incidents.
- \\ **Risk Management Team:** Incorporates threat intelligence into risk assessments and mitigation strategies.
- \\ **All Employees:** Required to report any suspicious activities or potential threats to the Threat Intelligence Team.

## Procedures

- \\ **Collection Procedures:** Define the methods and tools used for collecting threat intelligence.
- \\ **Analysis Procedures:** Outline the steps for analysing and validating threat intelligence.
- \\ **Dissemination Procedures:** Specify how and to whom threat intelligence will be communicated.
- \\ **Integration Procedures:** Describe how threat intelligence will be used in risk management and incident response.

## Compliance and Monitoring

Compliance with this policy shall be monitored through regular audits and assessments. Non-compliance may result in disciplinary action.

## Review and Revision

This policy shall be reviewed annually and updated as necessary to reflect changes in the threat landscape and organisational requirements.