

February 2025

INTERNAL

Incident Management Policy

FUNDS  AXIS

Policy title:	Incident Management Policy
----------------------	----------------------------

Issue	3.0
Approved by:	Trevor Dempster
Approval Date:	February 2025
Next Review Date:	February 2026

Scope:	The policy applies to Funds-Axis Limited and all contractors and other people working on behalf of the company.
Associated documentation:	<ul style="list-style-type: none"> \ Information Security & Technology Control Policy \ Quality Policy \ Client Support SLA
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"> \ Training
------------------------------	--

Introduction

This policy outlines the agreed procedures for managing and reporting significant incidents that affect company personnel, operations, assets, or customers. The aim is to ensure timely and effective responses to incidents and non-conformities, providing management visibility and enabling appropriate follow-up actions to mitigate future incidents. This policy also supports compliance with ISO 9001 and ISO 27001.

All incidents must be reported to the CISO and/or the Head of Assurance & Operational Risk as soon as possible and no later than the same day of the occurrence.

Definition of Incident

An **Incident** refers to any event that negatively impacts company personnel, operations, assets, or customers, or occurs on company premises. Incidents are managed through the company's formal **Incident Management System**.

Examples of incidents include:

- \ Non-fulfillment of a client requirement
- \ Non-compliance with ISO 9001 or ISO 27001
- \ Health and safety events (e.g., injuries in the office)
- \ Unauthorised access to IT systems
- \ Company system outages or data breaches
- \ Loss of assets (e.g., company laptops)
- \ Improper disposal of confidential information.

Incident Management Logging System (ServiceDesk Plus)

All incidents and non-conformities must be reported to the CISO and/or the Head of Assurance & Operational Risk as soon as possible. Incidents are logged in **ServiceDesk Plus** using the following procedure:

1. Raising an Incident Ticket:

- \ Open **ServiceDesk Plus** and click "New Incident."
- \ Fill in the fields as follows:
 - o **Request Type:** (Incident, Request for Information, Service Request)
 - o **Impact:** (Affects Business, Affects Department, Affects Group, Affects User)
 - o **Urgency:** (High, Low, Medium, Urgent)

- **Impacts Client SLAs:** (Yes, No)
- **Service Category:** (Automation, Cyber Security, HighWire, Infrastructure, Personal IT, Sisense, Other)
- **Issue Details:** Provide as much information and evidence as possible.

2. Classification of Incident:

- \ **Affects Business:** Major impact on the company, akin to previous "Critical."
- \ **Affects Department:** Significant impact, akin to previous "High."
- \ **Affects Group:** Medium impact, akin to previous "Medium."
- \ **Affects User:** Minor impact, akin to previous "Low."

3. Priority Levels:

- \ Tickets will be prioritised based on the predefined **SLA** framework as outlined in our **Client Support SLA document**.

Managing Incidents

Once logged in **ServiceDesk Plus**, the CISO or the Head of Assurance & Operational Risk is responsible for managing the incident, including investigating the issue, gathering evidence, and identifying the causes. Where applicable, ad-hoc director meetings will be held for significant incidents.

The following information must be included when creating the incident ticket:

- \ Subject: "INCIDENT –" followed by a brief descriptive heading.
- \ Description: Nature and description of the incident, names of affected persons, time/date of the incident, and the name of the senior management person reported to.
- \ Classification: Based on the impact on business, department, group, or user.

Incident Investigation, Treatment, and Reporting

The CISO or the Head of Assurance & Operational Risk is responsible for investigating and documenting evidence related to the incident. This includes:

- \ Gathering logs, system status information, or other evidence.
- \ Conducting interviews with staff or third parties as necessary.
- \ Drafting an action plan to prevent recurrence, which may include updating the ISMS or other systems.

All incidents are documented in **ServiceDesk Plus** with supporting evidence (e.g., screenshots, logs), and the action plan is tracked to resolution. Upon completion, the CISO or the Head of Assurance & Operational Risk will close the ticket.

Where necessary, relevant stakeholders, such as clients or regulators, will be informed of the outcome.

Considerations for Evidence Collection and Chain of Custody

In cases requiring the collection of first-hand evidence (e.g., log files), follow these best practices:

- \\ **Timely Collection:** Electronic evidence must be captured as soon as possible.
- \\ **Chain of Custody:** Ensure proper documentation of how the evidence was collected, handled, and stored to maintain its integrity for legal purposes.
- \\ **Uncontaminated Tools:** Use predefined tools for evidence collection to avoid tampering.
- \\ **Proper Logging:** All actions, including evidence collection and analysis, must be logged with a timestamp and a description of the activities.

Incident Closure

Once resolved, the incident will be closed in **ServiceDesk Plus**, and the individual who reported the incident will be notified. The CISO or the Head of Assurance & Operational Risk will periodically review actions to ensure effectiveness and prevent recurrence.

Responsibilities Summary

Individual/Governance Forum	Responsibility
Employee involved or witnessed	Inform CISO and/or Head of Assurance & Operational Risk and provide full information
CISO / Head of Assurance & Operational Risk	Log incident in ServiceDesk Plus and manage investigation/action
CISO / Head of Assurance & Operational Risk	Allocate individual responsibilities for remedial actions
Platform Meeting / Board Meeting	Overall monitoring and control of incidents through review logs
CISO / Head of Assurance & Operational Risk	Periodic review of incident responses and preventive measures