INFORMATION SECURITY

Information Security Policy

Version 1.3

Status	PUBLISHED
Classification	Restricted
Date Updated	01/09/2026
Version	1.3

This document is classified as RESTRICTED

Document Control

Revision history

Date	Version	Author	Summary of changes
19/04/2017	1.0	Rahim Hankin	Version 1 issued
06/02/2026	1.1	Reuben Njoku	Complete review by VCISO
08/06/2026	1.2	Muji Ali	Amended applicability
22/06/2026	1.3	Muji Ali	Title Amended to Information Security Policy

Approvals

Date	Version	Approver name	Approver title
13/02/2026	1.1	Rahim Hankin	Technical Director
08/06/2026	1.2	Muji Ali	Information Security Lead
01/09/2026	1.3	Muji Ali	Information Security Lead

Table of Contents

1	Purpose
2	Management Commitment
3	Scope of the ISMS
4	Information Security Objectives
5	Governance and Accountability
6	Policy Framework
7	Compliance and Continual Improvement
8	Communication
9	Review
10	Approval and Signatures

1. Purpose

This policy sets out the formal commitment of senior management to establish, implement, maintain, and continually improve an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022.
The ISMS exists to protect FDM UK's information assets and to support the organisation's business objectives, client commitments, and regulatory obligations.

2. Management Commitment

Senior management of FDM UK is fully committed to information security and recognises that effective protection of information is essential to maintaining trust, reputation, and operational resilience.
Management commits to:

- protecting the confidentiality, integrity, and availability of information handled by FDM UK
- ensuring information security objectives are established, monitored, and aligned with the organisation's strategic direction
- integrating information security requirements into business processes, technology operations, and ways of working
- providing appropriate resources, authority, and support to operate and improve the ISMS
- ensuring that applicable legal, regulatory, contractual, and client requirements are identified and met
- promoting a strong information security culture through awareness, training, and accountability
- supporting continual improvement through risk management, monitoring, internal audits, management reviews, and corrective actions

3. Scope of the ISMS

The ISMS applies to:

- all FDM UK employees, contractors, and relevant third parties
- information in all forms, including electronic, physical, and verbal
- the systems, services, platforms, and supporting processes used to deliver FDM UK's business activities and client services

The detailed scope of the ISMS is defined and maintained as documented information within the ISMS.

4. Information Security Objectives

FDM UK's information security objectives include:

- preventing unauthorised access to sensitive business, client, and personal information
- ensuring the accuracy and integrity of data, analysis, and research outputs
- maintaining availability and resilience of critical systems and services
- detecting, responding to, and learning from information security incidents
- managing information security risks in a structured and proportionate manner

Objectives are reviewed regularly as part of the ISMS governance process.

5. Governance and Accountability

- Senior management retains ultimate accountability for the effectiveness of the ISMS.
- The VCISO/ ISMS Manager/Operations Manager is responsible for maintaining the ISMS framework, reporting on its performance, and coordinating assurance activities.
- System owners and managers are responsible for implementing and operating controls within their areas.

- All personnel are responsible for complying with ISMS policies and reporting security concerns or incidents promptly.

6. Policy Framework

This ISMS Policy is supported by a framework of subordinate policies, standards, and procedures, including but not limited to:

- Information Security Policy
- IT Acceptable Use Policy
- Technology Security Policy
- Information Handling Policy
- Access Control and Authentication Policies
- Incident Response and Business Continuity Plans

Together, these documents define how information security is implemented and enforced across FDM UK.

7. Compliance and Continual Improvement

FDM UK will:

- monitor and measure ISMS performance
- conduct internal audits and management reviews at planned intervals
- address nonconformities through corrective actions
- continually improve the suitability, adequacy, and effectiveness of the ISMS

8. Communication

This policy is communicated to all personnel working under the control of FDM UK and is made available to relevant interested parties where appropriate, including auditors and clients.

9. Review

This policy is reviewed at least annually and whenever significant changes occur to the organisation, technology environment, risk landscape, or regulatory requirements.

10. Approval

This policy is approved by senior management and demonstrates FDM UK's commitment to maintaining an effective Information Security Management System.

Approved by:
Name: Rahim Hankin

Signature:
Title: Co-Founder
Date: 03/09/2026

Acknowledged by:
Name: Muji Ali
Title: Information Security Lead/VCISO
Signature: Muji Ali
Date: 03/09/2026