

Document Title: Integrated Management System Policy
Document No: MDT-IMS-PY-001
Revision: 3
Date: 5th December 2024

DOCUMENT INFORMATION

REVISION HISTORY

Rev	Date	Description	Created By	Reviewed By	Approved By
A	28/09/2022	Draft for internal review	QHSE Aberdeen	DYM	-
0	18/11/2022	Approved for use	QHSE Aberdeen	DYM	DYM
1	09/02/2023	Approved for use	QHSE Aberdeen	DYM	DYM
2	12/02/2024	Approved for use	QHSE Aberdeen	DJM	DYM
3	05/12/2024	Approved for use	DYM	DJM	APB

AMENDMENT RECORD

Revision	Description of Changes
1	Amended to include quality requirements
2	Reviewed at MRM. No changes to content. Re-signed.
3	All sections updated to comply with ISO 27001:2022 and classification added.

DISCLAIMER

This document is intended for the sole use of the person or company to whom it is addressed, and no liability of any nature whatsoever shall be assumed to any other party in respect of its contents. As to the addressee, MITOSIS DIGITAL TECHNOLOGIES LTD (the Company) shall not be liable for any loss or damage whatsoever suffered by virtue of any act, omission, or default (whether arising by negligence or otherwise) by the Company or any of its servants.

CONTENTS

DOCUMENT INFORMATION	2
1. PURPOSE	4
2. SCOPE	4
3. POLICY	4
3.1 Quality Management	4
3.2 Information Security Management	4
3.3 Integration of Quality and Information Security	4
3.4 Employee Responsibilities	4
3.5 Continuous Improvement	4
4. KEY OBJECTIVES	5
5. RESPONSIBILITIES	5

1. PURPOSE

This Integrated Management System (IMS) Policy outlines Mitosis Digital Technologies' commitment to quality and information security by integrating the principles of ISO 9001:2015 (Quality Management) and ISO 27001:2022 (Information Security Management). It demonstrates our dedication to delivering high-quality services while safeguarding information assets, meeting customer and stakeholder needs, and continually improving our systems and processes.

2. SCOPE

This policy applies to all business operations, employees, contractors, and third parties engaged in delivering products or services, managing information assets, or contributing to the company's management systems. It encompasses:

- Quality Management (aligned with ISO 9001:2015)
- Information Security Management (aligned with ISO 27001:2022)

3. POLICY

It is our policy to comply with the following statements.

3.1 Quality Management

- Consistently meet or exceed customer expectations by delivering high-quality products and services.
- Comply with applicable statutory, regulatory, and contractual requirements.
- Foster a culture of continuous improvement in all processes.
- Regularly assess customer feedback to enhance satisfaction and drive innovation.

3.2 Information Security Management

- Protect the confidentiality, integrity, and availability of all information assets.
- Identify and address information security risks through a structured risk assessment process.
- Comply with legal, regulatory, and contractual obligations related to information security.
- Implement controls such as encryption and access management to safeguard sensitive information.

3.3 Integration of Quality and Information Security

- Align processes to ensure seamless management of quality and information security.
- Use risk-based thinking to address challenges affecting quality or information security objectives.
- Maintain documentation and evidence to support compliance with ISO 9001:2015 and ISO 27001:2022.

3.4 Employee Responsibilities

- Require all employees and contractors to adhere to this policy and related procedures.
- Provide training to ensure awareness of quality and information security principles.
- Encourage employees to report incidents, risks, or non-conformities promptly.

3.5 Continuous Improvement

- Monitor and measure the performance of quality and information security management systems through audits, reviews, and key performance indicators (KPIs).
- Regularly update processes and controls to address emerging risks, regulatory changes, and stakeholder feedback.
- Foster a culture of innovation and excellence to drive continual improvement in all areas of the IMS.

4. KEY OBJECTIVES

To achieve this policy, Mitosis Digital Technologies is committed to the following objectives:

- Deliver services that consistently meet or exceed customer expectations.
- Protect information assets from unauthorised access, breaches and data loss.
- Ensure compliance with applicable statutory, regulatory, and contractual requirements.
- Maintain a customer satisfaction score of 90%.
- Conduct regular information security awareness training for all employees.
- Perform periodic risk assessments and ensure treatment plans are implemented within agreed timelines.

5. RESPONSIBILITIES

We assign responsibilities to:

- Top Management:
 - To ensure the IMS aligns with the organisation's strategic direction and goals.
 - Promote a culture of quality and information security throughout the organisation.
- IMS Manager:
 - To oversee the implementation, monitoring, and improvement of the IMS.
 - To ensure compliance with ISO 9001:2015 and ISO 27001:2022 requirements.
- Employees and Contractors:
 - To adhere to IMS policies and procedures.
 - To actively participate in training programmes and report non-conformities or security incidents.

Mitosis Digital Technologies senior management ensures that our policies, commitments and aims are achieved through the establishment of Specific, Measurable, Achievable, Realistic and Timebound (SMART) objectives.

Mitosis Digital Technologies aims to achieve its legal obligations, policy commitments and objectives through review and continuous improvement of the IMS, communication, competent personnel and appropriate supervision.