

ISMS Policy

Code:	MCR-ICT-ISM-001
Version:	1.5
Date of version:	29/07/2024
Created by:	Jonathan Simpson
Reviewed by:	Alwyn Dormehl
Approved by:	Gerhardt Van Der Merwe
Confidentiality level:	Confidential

Change history

Date	Version	Created by	Description of change
20/02/2019	1.0	Jonathan Simpson	Document initiation
31/08/2020	1.1	Jonathan Simpson	Annual review
01/03/2021	1.2	Jonathan Simpson	Updated ISMS Statement
16/08/2022	1.3	Jonathan Simpson	Updated document control
03/03/2023	1.4	Jonathan Simpson	Annual review
29/07/2024	1.5	Jonathan Simpson	Annual review

Table of contents

1. REFERENCE

2. ISMS POLICY STATEMENT

3. VALIDITY AND DOCUMENT MANAGEMENT

2

2

3

1. Reference

Standard	Title	Description
ISO 27000:2014	Information security management systems	Overview and vocabulary
ISO 27001:2013	Information security management systems	Requirements
ISO 27002:2013	Information technology - security techniques	Code of practice for information security controls

2. ISMS Policy Statement

“Establish, monitor and continually improve our safeguards for the confidentiality, integrity and availability of all physical and electronic information assets to ensure that regulatory, operational and contractual requirements are fulfilled.”

The Policy ensures and guarantees that:

- **Confidentiality:** Confidentiality of information shall be kept. Information shall not be disclosed to unauthorized persons on any accidental or deliberate actions.
- **Integrity:** Integrity of information shall be maintained by ensuring protecting against unauthorized access. Information shall be complete and accurate.
- **Availability:** Information shall be available and delivered to the right person, at the time when it is needed. Make information available to authorized business processes and employees when required.
- Policy is supported through Business Continuity Plan, which will be defined, maintained and tested in continuous practical work.
- All Information security violations will be reviewed, documented and investigated.
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies.
- Organization Comply to all applicable laws and regulations and contractual obligations related to information security.

This policy governs our day-to-day operations to ensure the security of information and is communicated and implemented throughout our organization. Our Information Security Policy is made available as a stand-alone document and widely distributed, including during induction.

Our Information Security Policy is typically reviewed annually, as part of our information security management review program, or as required to recognize the changing needs and expectations of relevant interested parties or the risks and opportunities identified by the risk management process.

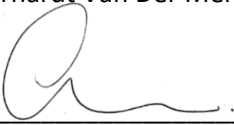
3. Validity and document management

This document is valid as of 29 July 2024.

The owner of this document is the ICT Manager and the reviewer is the Practice Manager, who must check and, if necessary, arrange for the update of the document at least once a year.

The Chairman of MacRobert Attorneys Board approves Policies.

Board Chairman
Gerhardt Van Der Merwe



Signature

30 July 2024

Date