MIOD IT GOVERNANCE POLICY

1. PURPOSE AND CONTEXT

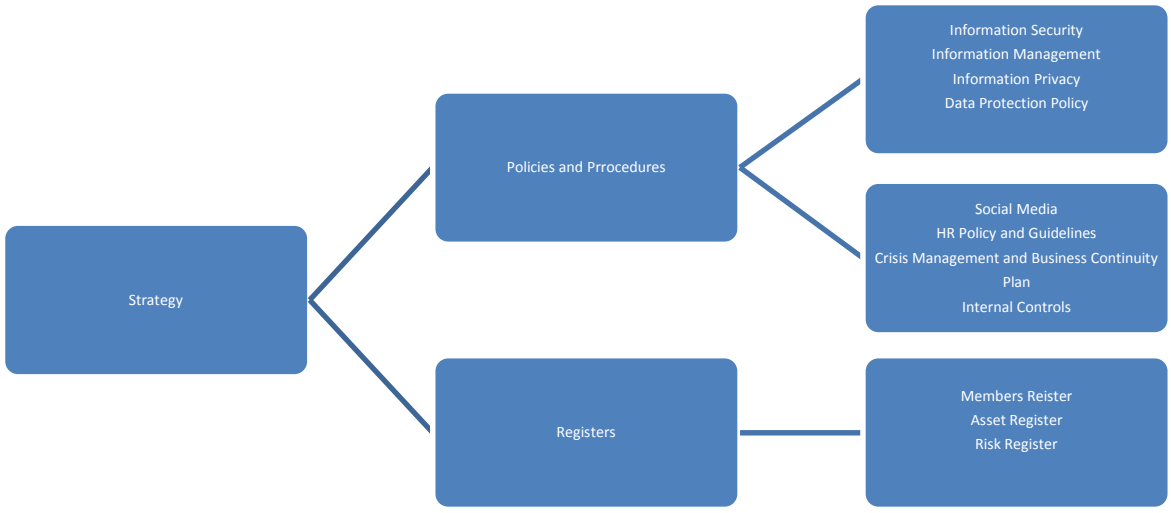
The MIOD's prime objective is to promote good corporate governance and best business practices as well as being a role model. It is the role of the Board to ensure that procedures and practices are in place to protect the company's assets and reputation. Information technology has a profound effect on processes within the organisation and it is therefore essential for the MIOD to have a sound IT Governance Policy in place in line with legal requirements and the Code of Corporate Governance.

2. KEY PRINCIPLES

- The board is responsible for IT governance and ensures that the appropriate policies and procedures are in place in line with applicable laws, codes and best practice
- The board will adopt an IT governance framework and ensure that it is implemented
- IT should be aligned with the company's performance and sustainability objectives
- The Board will monitor and evaluate significant IT investments and expenditure
- IT forms an integral part of the MIOD's risk management
- The board will ensure that there are systems in place for the management of information which will include information security, information management and information privacy;
- The board will ensure that the necessary skills are in place so that their responsibilities in respect of internal control systems are adequately discharged
- The board should receive from time to time independent assurance on the effectiveness of the IT internal controls

3. FRAMEWORK AND SCOPE

The IT Governance Framework summarises the manner in which IT is governed at the MIOD:



Scope:

-All types of information on all types of media, communications and access technologies

-All MIOD IT assets

4. STRATEGY

The MIOD seeks to be a role model of corporate governance and our strategy is therefore to create and maintain a highly reliable and secure Information Technology environment to ensure the reputation, integrity and sustainability of the organisation.

5. RESPONSIBILITY

- The Board:
    - Continually improves the organisation's IT governance infrastructure
    - Ensures that IT and IT-enabled strategic plans are aligned with organisational objectives
    - Ensures that adequate IT resources are available to meet the organisation's strategic objectives
    - Ensures the return on investment from significant IT and IT-enabled projects
    - Approves the IT Governance Policy and Framework, reviews it annually and delegates its responsibility as follows:

- The Audit and Risk Committee:
    - Assists the board in its IT responsibilities
    - Reviews the legal risks and ensures compliance with applicable laws, codes and best practice
    - Reviews IT risk identification and management
    - Ensures that IT risks are adequately addressed. In understanding and measuring IT risks, the members of the committee should understand the company's overall exposure to IT risks from a strategic and business perspective, including the areas of the business that are most dependent on IT for effective and continual operation
    - Obtains appropriate assurance that controls are in place and effective in addressing IT risks
    - Considers IT as it relates to financial reporting and the going concern of the company
    - Ensures that the Business Continuity System is current and effective

- Management is responsible for:
    - Implementing the IT Governance Framework
    - Providing accurate and timely reports
    - Acting within the bounds provided by the policies and delegated authorities
    - Acting within authorized financial limits
    - Managing compliance
    - Monitoring IT service delivery and the achievement of agreed service levels
    - Continually improving the organisation's management of information
    - Continually improving the organisation's IT security infrastructure

6. IT POLICIES

For each policy there will be a standard and a procedure with a specified target user group.

Scope:
The policies cover the MIOD's management information systems, its IT security and confidentiality and privacy, including how employees create, access, store, and dispose of information whether of a personal or business nature. It covers all the information assets held by the organisation, including emails and social media.

List of policies:	
• Accessibility and Disclosure	• Covered by Data Protection Policy
• Bring Your Own Device (BOYD)	• BOYD Policy (new)
• Building security and access	
• Computer, Email and Internet Use	• Covered by HR Policy
• Confidentiality and Privacy	• Covered by HR Policy and Data Protection Policy
• Crisis Management and Business Continuity Plan	• Crisis Management and Business Continuity Plan
• Data Protection	• Data Protection Policy
• Employee conduct	• Covered by HR Policy
• Email and Instant Messaging	• Covered by HR Policy
• Equipment requests (Adds, Changes, Deletes)	
• Intellectual Property and Copyright	
• Internet usage	• Covered by HR Policy
• Information Management	
• Inventory and equipment	
• IT Security	
• Password Security	• Password Security Policy (new)
• PC software standards	• Covered by HR Policy
• PC standards	
• Phone usage	• Covered by HR Policy
• Registers	
• Remote access	
• Reporting	
• Reviews	
• Service level agreements	
• Social Media	• Social Media Policy (new)
• Software usage	
• Use and Release of Information- Public Comment	• Covered by Data Protection Policy
• Use of Company Resources	• Covered by HR Policy
• Working from Home	