# ISMS Policy Statement

Classification: Public

## Document Details

| | |
|---|---|
| Original Approval Date | 07/02/2024 |
| Original Approval Authority | Regional CEO |
| Date Approved/Last Reviewed: | February 2025 |
| Policy Owner: | GCISO |
| Contact Person: | GCISO |
| Functional Applicability & Audience: | All I&M Group and its interested parties |
| Current Revision Date: | February 2026 |
| Date Approved: | February 2025 |
| Next Review Date: | February 2027 |
| Version: | 1.3 |
| Notes | The policy was reviewed; no changes required |

## I&M Group Information Security Policy Statement

I&M Group is a leading corporate group in East Africa, with a major presence in Banking, Insurance and Real Estate. The Group offers a full range of personal, business and alternate banking channels through its presence in Kenya, Tanzania, Rwanda, Mauritius and Uganda.

| Our Aspiration | Vision | Mission |
|---|---|---|
| **To be Eastern Africa's Leading Financial Partner for Growth** | To become a company where the best people want to work, the first choice where customers want to do business and where shareholders are happy with their investment | To become partners of growth for all our stakeholders by meeting our customers' expectations, motivating and developing every employee and enhancing shareholder value |

Senior Management places the highest priority on safeguarding information in every aspect. We recognize that as an organization, we have the ability to mitigate information security risks by upholding the confidentiality, integrity, and availability of information. This assurance instils confidence among stakeholders that risks stemming from potential incidents are effectively addressed. Our overarching objective is to consistently enhance the performance of our Information Security Management System (ISMS) throughout the business.

In order to achieve this, the following information security objectives have been established:

1. Manage the User - Keep user rights and privileges under control, allowing seamless productivity as the Bank engages in digitization and employs user education and awareness to ensure cyber risk is well understood by all stakeholders, who work hand in hand to manage this risk. This also includes having an innovative and growing cyber-security team underpinned by global best practices.
2. Protect the ICT Infrastructure - Become a hard target for all forms of aggression in cyberspace by utilizing modern technology to protect its ICT infrastructure. The Bank shall ensure that access to its ICT infrastructure is restricted to authorized persons and entities only, in accordance with approved access control requirements.
3. Respond to Threats - Own the means to respond to ever evolving cyber-threats against the Bank, to respond effectively to incidents, to ensure the Bank's networks, data and systems are protected and resilient. The Bank will detect, understand, investigate and disrupt hostile action, pursuing and presenting offenders to relevant bodies for prosecution. The Bank will also work to ensure that its staff and clients have the knowledge and ability to defend themselves.

To achieve these objectives, we shall act to:

- Make sure information is protected to an appropriate level, based upon its classification and impact of its disclosure, modification, or loss.

- Complying with all relevant information management legislation, regulations and standards.
- Make sure that employees are clear about their responsibilities regarding ownership of information security, and that we expect them to take their legal and moral role seriously.
- Assign the necessary authority for the management, operation, and reporting of ISMS performance.
- Ensure that the resources needed for the ISMS are available.
- **Maintaining an ISMS which meets** the requirements of ISO 27001:2022.
- This policy, together with the objectives and targets set, will be reviewed on an annual basis to ensure that it remains relevant and suitable for operations of the I&M Group.

| **SIGNED BY** | **DATE** |
|---|---|
| Kihara Maina,<br>*Regional Chief Executive Officer* | 26/02/2025 |