ENERGY REGULATED NON-WDT SACCO SOCIETY LTD

# RISK MANAGEMENT POLICY

August 2025

## 1. PURPOSE

The purpose of this Risk Management Policy is to establish a structured framework through which **Energy RNWDT Sacco** identifies, assesses, monitors, and mitigates risks that may impact its financial stability, operational efficiency, compliance obligations, and reputation. The policy aligns with the **Co-operative Societies Act, Cap 490**, the **Sacco Societies Act and Regulations (SASRA)**, and relevant national laws to ensure member funds and institutional assets are safeguarded at all times.

Specifically, this policy seeks to:

i. **Protect Member Assets:** Safeguard members' savings, deposits, and investments against losses arising from financial mismanagement, fraud, or external shocks.
ii. **Ensure Regulatory Compliance:** Provide a clear framework for complying with SASRA prudential standards, the Co-operative Societies Act, and other statutory obligations including tax, AML/CFT, and data protection laws.
iii. **Promote Sound Governance:** Embed risk management in governance structures and decision-making processes of the Board, Supervisory Committee, Credit Committee, and management.
iv. **Enhance Operational Resilience:** Strengthen the Sacco's capacity to withstand financial, technological, or reputational shocks and recover from crises.
v. **Support Strategic Growth:** Facilitate informed decision-making and sustainable growth by anticipating risks and aligning them with the Sacco's strategic plan.
vi. **Build Member Confidence:** Maintain transparency and accountability in risk management, thereby enhancing trust among members, regulators, and partners.
vii. **Mitigate Emerging Risks:** Proactively address new risks such as cybersecurity, climate change, political instability, and economic fluctuations that may impact Sacco operations.

Ultimately, the purpose of this policy is to ensure that risk management becomes an **integral part of the Sacco's culture**, enabling proactive prevention and effective response to risks while ensuring sustainable service delivery and long-term financial health.

## 2. SCOPE

This Risk Management Policy applies to **all aspects of Energy RNWDT Sacco's operations, governance, and relationships**. It establishes a unified approach to managing risks across financial, operational, compliance, technological, and strategic dimensions.

### 2.1 Organizational Scope

The policy binds the following stakeholders:

- **Board of Directors** – responsible for overall risk governance and policy oversight.

- **Supervisory Committee** – responsible for independent oversight and internal controls.
- **Credit Committee** – responsible for prudent credit administration and loan portfolio management.
- **Management and Employees** – responsible for day-to-day implementation of risk controls.
- **Members** – responsible for providing accurate information, complying with Sacco policies, and safeguarding their own interactions with the Sacco.
- **External Stakeholders** – including service providers, auditors, consultants, and partners who process or handle Sacco data, finances, or operations under binding contracts.

### 2.2 Risk Coverage

The policy covers **all categories of risks** that may affect the Sacco, including but not limited to:

i. **Strategic Risks** – arising from poor planning, weak governance, or external policy changes.
ii. **Financial Risks** – including credit risk, liquidity risk, interest rate risk, capital adequacy, and investment risk.
iii. **Operational Risks** – related to processes, people, systems, or internal controls.
iv. **Compliance & Legal Risks** – arising from non-adherence to SASRA regulations, the Co-operative Societies Act, POCAMLA (2009), and other applicable laws.
v. **Reputational Risks** – arising from governance failures, fraud, or negative publicity.
vi. **Technology & Cybersecurity Risks** – system breakdowns, cyberattacks, data breaches, or ICT failures.
vii. **Environmental, Social, and Governance (ESG) Risks** – linked to sustainability, ethics, and social responsibility.
viii. **External Risks** – macroeconomic changes, political instability, or pandemics.

### 2.3 Operational Scope

The policy applies to **all Sacco processes**, including but not limited to:

- Membership recruitment and services.
- Savings and deposit management.
- Credit/loan approval, disbursement, monitoring, and recovery.
- Investment and liquidity management.
- Procurement and vendor management.
- ICT and data protection management.
- Human resource and staff welfare management.
- Regulatory and statutory reporting.

### 2.4 Geographic Scope

This policy applies to all Sacco operations within Kenya and extends to any cross-border transactions or services where Energy RNWDT Sacco engages with foreign institutions, partners, or technology platforms.

## 3. OBJECTIVES

The primary objective of this Risk Management Policy is to **provide a structured and proactive approach** for managing risks that may threaten the sustainability, stability, and growth of Energy RNWDT Sacco. The policy seeks to institutionalize risk management as a core governance and operational function.

### 3.1 Strategic Objectives

i. **Safeguard Member Wealth:** Protect members' savings, deposits, and investments by ensuring robust internal controls and prudent financial practices.
ii. **Strengthen Governance:** Provide a clear framework for the Board, Supervisory Committee, and management to oversee and manage risks in compliance with cooperative governance principles.
iii. **Ensure Regulatory Compliance:** Align Sacco operations with requirements of the **Co-operative Societies Act, Sacco Societies Act, SASRA Regulations, POCAMLA (2009)**, and other applicable national laws.
iv. **Support Strategic Planning:** Enable risk-informed decision-making that aligns with the Sacco's strategic plan and long-term vision.

### 3.2 Operational Objectives

i. **Embed a Risk Culture:** Foster awareness and accountability at all organizational levels so that risk management becomes part of everyday operations.
ii. **Identify and Assess Risks:** Establish systems for early identification, analysis, and evaluation of risks across financial, operational, compliance, and external domains.
iii. **Implement Mitigation Measures:** Develop preventive and corrective actions to minimize the probability and impact of identified risks.
iv. **Enhance Operational Resilience:** Ensure business continuity by preparing for crises such as loan defaults, liquidity crunches, ICT disruptions, or external shocks.

### 3.3 Monitoring and Accountability Objectives

i. **Regular Monitoring:** Ensure continuous monitoring of the risk environment, with timely reporting to the Board and regulators.
ii. **Transparency and Disclosure:** Promote open communication on risk exposures and mitigation strategies to members, auditors, and regulators.

iii. **Continuous Improvement:** Review and update risk frameworks regularly to incorporate emerging risks such as cybersecurity, climate change, and digital finance.

iv. **Stakeholder Confidence:** Reinforce member trust and external stakeholder confidence by demonstrating robust risk management practices.

## 4. RISK MANAGEMENT PRINCIPLES

Energy RNWDT Sacco shall be guided by universally accepted risk management standards, SASRA prudential guidelines, and cooperative principles in implementing this policy. These principles ensure that risk management is not a one-off activity but a continuous, organization-wide practice.

### 4.1 Accountability and Oversight

- The **Board of Directors** holds ultimate responsibility for risk governance, supported by the Supervisory Committee and management.
- Clear lines of accountability shall be established so that every officer, staff member, and committee is aware of their role in managing risks.

### 4.2 Integration into Operations

- Risk management shall be embedded into all Sacco processes — from **strategic planning, credit operations, savings mobilization, procurement, ICT management,** to **regulatory compliance.**
- All business decisions must incorporate a risk assessment to balance potential benefits against possible exposures.

### 4.3 Proportionality

- Risk responses shall be proportional to the likelihood and impact of the identified risks.
- High-impact risks (e.g., liquidity shortfalls, loan defaults, cyber breaches) shall be prioritized for immediate mitigation, while low-impact risks may be managed through monitoring.

### 4.4 Transparency and Communication

- Risk identification, reporting, and management shall be conducted openly and objectively.
- Members, regulators, and other stakeholders shall be informed of material risks and the measures taken to address them, in line with cooperative values of openness and accountability.

### 4.5 Compliance with Legal and Regulatory Requirements

- All risk management practices must comply with the **Co-operative Societies Act, SASRA Regulations, POCAMLA (2009), Data Protection Act (2019),** and other applicable national legislation.

- Non-compliance with statutory requirements shall be treated as a critical risk to be immediately addressed.

### 4.6 Continuous Monitoring and Improvement

- Risks shall be continuously assessed given the dynamic financial, technological, and regulatory environment.
- The Sacco shall regularly review and update its risk management framework to address emerging threats such as **cybersecurity attacks, fintech disruptions, and climate change impacts.**

### 4.7 Member-Centric Approach

- As a cooperative, all risk management practices shall prioritize the **protection of members' funds and interests.**
- Decisions shall always align with cooperative values of self-help, responsibility, democracy, and solidarity.

## 5. RISK CATEGORIES

Energy RNWDT Sacco recognizes that risks arise from both internal and external environments, and they must be categorized for systematic management. The following risk categories apply to the Sacco:

### 5.1 Strategic Risks

- **Definition:** Risks that arise from inappropriate business strategies, poor governance, inadequate succession planning, or failure to adapt to changing environments.
- **Examples in Sacco Context:**
    - Misalignment between strategic plan and member needs.
    - Weak leadership or governance lapses in the Board or Committees.
    - Failure to diversify income sources.
    - Ignoring emerging opportunities such as green financing or digital platforms.

### 5.2 Financial Risks

- **Definition:** Risks associated with the Sacco's financial health, sustainability, and member funds.
- **Types:**
    - **Credit Risk:** Member loan defaults, poor loan appraisal, over-concentration in high-risk sectors.
    - **Liquidity Risk:** Inability to meet members' withdrawal requests or loan disbursements due to poor cash flow.
    - **Interest Rate Risk:** Adverse impact from fluctuating interest rates on loans and deposits.
    - **Capital Adequacy Risk:** Failure to maintain SASRA-required capital ratios.

- **Investment Risk:** Poor investment decisions leading to financial losses.

### 5.3 Operational Risks

- **Definition:** Risks arising from internal processes, systems, or human actions.
- **Examples:**
  - Errors in loan processing or record-keeping.
  - Staff fraud, collusion, or misappropriation of funds.
  - Inadequate segregation of duties.
  - Weaknesses in ICT systems or internal controls.
  - Disruption of operations due to strikes, accidents, or natural disasters.

### 5.4 Compliance & Legal Risks

- **Definition:** Risks of penalties, fines, or sanctions due to non-compliance with laws, regulations, or internal policies.
- **Examples:**
  - Breach of SASRA prudential standards (e.g., liquidity or capital adequacy ratios).
  - Failure to comply with **AML/CFT requirements** under POCAMLA (2009).
  - Non-adherence to the **Data Protection Act (2019)** in handling member data.
  - Breach of tax laws and statutory obligations.

### 5.5 Reputational Risks

- **Definition:** Risks that damage the Sacco's credibility, image, or stakeholder trust.
- **Examples:**
  - Negative publicity due to fraud or member complaints.
  - Poor customer service leading to member dissatisfaction.
  - Failure to communicate transparently with members and regulators.
  - Governance scandals or leadership wrangles.

### 5.6 Technology & Cybersecurity Risks

- **Definition:** Risks from reliance on ICT systems and digital platforms.
- **Examples:**
  - Data breaches, hacking, or phishing attacks.
  - System downtimes or outages disrupting member services.
  - Fraud through mobile banking or online channels.
  - Inadequate data backup or disaster recovery mechanisms.

### 5.7 Environmental, Social, and Governance (ESG) Risks

- **Definition:** Risks linked to environmental sustainability, social responsibility, and governance practices.
- **Examples:**
  - Climate change effects on loan repayment capacity (e.g., agricultural loans affected by drought).

- Failure to uphold gender inclusivity or ethical lending practices.
- Poor governance leading to conflict of interest or mismanagement.

### 5.8 External Risks

- **Definition:** Risks outside the Sacco's direct control but with potential significant impacts.
- **Examples:**
  - Economic downturns, inflation, or exchange rate volatility.
  - Political instability or regulatory shifts.
  - Pandemics and global shocks affecting members' ability to repay loans or save.
  - Competition from banks, fintechs, or other SACCOs.

## 6. RISK MANAGEMENT FRAMEWORK

Energy RNWDT Sacco shall adopt a **systematic and continuous framework** for managing risks. This framework ensures that risks are identified early, assessed objectively, mitigated effectively, and monitored continuously. It follows a **four-step cycle** consistent with SASRA prudential standards and international risk management best practices.

### 6.1 Risk Identification

i. **Objective:** To recognize and document all potential risks that could affect Sacco operations, finances, or reputation.
ii. **Approach:**
   a. Regular risk assessments at Board, management, and departmental levels.
   b. Use of tools such as **risk registers, checklists, scenario planning, and member feedback.**
   c. Inclusion of emerging risks such as **cybersecurity threats, climate-related risks, and fintech disruptions.**
iii. **Responsibility:** Risk identification is a shared responsibility across all staff, committees, and the Board, coordinated by the CEO and Risk Management Committee.

### 6.2 Risk Assessment

i. **Objective:** To evaluate the likelihood and potential impact of identified risks.
ii. **Methodology:**
   a. Risks shall be assessed using a **Risk Matrix** (Low/Medium/High probability vs. Low/Medium/High impact).
   b. Each risk shall be ranked to prioritize mitigation actions.
   c. Both **quantitative measures** (e.g., loan default rates, liquidity ratios) and **qualitative measures** (e.g., reputational damage, compliance gaps) shall be applied.
iii. **Output:** A risk profile that highlights **high-priority risks** requiring immediate attention.

### 6.3 Risk Mitigation

i. **Objective:** To reduce risk exposure through preventive, corrective, or transfer measures.
ii. **Strategies:**
    a. **Avoidance:** Stopping activities that create unacceptable risks.
    b. **Reduction:** Implementing controls to minimize probability or impact (e.g., internal controls, staff training, ICT safeguards).
    c. **Transfer:** Sharing risk through insurance or outsourcing to qualified service providers.
    d. **Acceptance:** Retaining risk at manageable levels, with monitoring.
iii. **Example in Sacco context:**
    a. Strengthening loan appraisal and monitoring to reduce credit risk.
    b. Purchasing fidelity insurance to cover staff fraud.
    c. Maintaining liquidity buffers to manage liquidity risks.

### 6.4 Risk Monitoring and Reporting

i. **Objective:** To track risk exposures and ensure accountability.
ii. **Mechanisms:**
    a. Maintenance of a **Risk Register** updated quarterly.
    b. Regular reporting of risks and mitigation progress to the **Board of Directors.**
    c. Independent review by the **Supervisory Committee and internal auditors.**
    d. Annual disclosure of material risks to members at the AGM, in line with cooperative principles of transparency.
    e. Submission of compliance and risk reports to **SASRA** as required.

### 6.5 Continuous Improvement

i. The framework shall remain **dynamic** and responsive to changes in the business environment.
ii. Lessons learned from incidents, audits, and member feedback shall be incorporated into updated controls and processes.
iii. The Sacco shall benchmark against **sector best practices** and adopt modern tools (e.g., early warning systems, fintech risk dashboards).

## 7. RISK MITIGATION STRATEGIES

Energy RNWDT Sacco shall adopt targeted strategies to manage risks across all categories. Mitigation measures shall be **proactive, cost-effective, and aligned with SASRA regulations, the Co-operative Societies Act, and sector best practices.**

### 7.1 Governance and Strategic Risk Mitigation

i. Establish clear governance structures with **defined roles and responsibilities** for the Board, Committees, and Management.
ii. Undertake periodic **Board and Committee evaluations** to ensure effectiveness.
iii. Implement a **succession planning framework** for leadership continuity.
iv. Align strategic plans with **member needs, regulatory changes, and market dynamics.**
v. Conduct annual **strategic risk reviews** to adapt to emerging challenges.

### 7.2 Financial Risk Mitigation

i. **Credit Risk:**
   a. Strict loan appraisal and approval procedures.
   b. Credit scoring systems, guarantor requirements, and collateral policies.
   c. Regular monitoring of loan performance and arrears management.
   d. Diversification of loan portfolio to reduce concentration risks.
ii. **Liquidity Risk:**
   a. Maintain minimum liquidity ratios as per SASRA regulations.
   b. Establish contingency liquidity lines (e.g., external financing arrangements).
   c. Conduct regular **cash flow forecasting** to anticipate needs.
iii. **Interest Rate Risk:**
   a. Review lending and deposit rates periodically.
   b. Align rates with market trends while protecting Sacco sustainability.
iv. **Capital Adequacy Risk:**
   a. Maintain regulatory capital ratios.
   b. Build reserves through prudent surplus retention.
v. **Investment Risk:**
   a. Adopt conservative investment policies in line with SASRA guidelines.
   b. Seek Board approval for all investments and review performance quarterly.

### 7.3 Operational Risk Mitigation

i. **Internal Controls:** Implement segregation of duties, approval hierarchies, and audit trails.
ii. **Fraud Prevention:** Conduct staff background checks, rotate duties, and install whistleblowing mechanisms.
iii. **ICT Controls:** Enforce system access controls, backups, and disaster recovery systems.
iv. **Human Resource Risk:** Provide continuous training, fair HR policies, and enforce a staff code of conduct.
v. **Business Continuity:** Maintain a Business Continuity Plan (BCP) to respond to disasters and emergencies.

### 7.4 Compliance and Legal Risk Mitigation

i. Establish a **compliance unit** or designate a Compliance Officer.
ii. Conduct regular compliance audits against **SASRA, AML/CFT, and Data Protection Act requirements.**
iii. Ensure all statutory filings, tax obligations, and regulatory submissions are made on time.

iv. Train staff and Board on emerging laws and regulations affecting SACCOs.

### 7.5 Reputational Risk Mitigation

i. Foster a **culture of transparency, integrity, and ethical behavior.**
ii. Implement a **member service charter** with clear service standards.
iii. Address member complaints promptly through grievance redress mechanisms.
iv. Maintain proactive public relations and media engagement.
v. Disclose key risk issues and financial performance openly at the AGM.

### 7.6 Technology and Cybersecurity Risk Mitigation

i. Deploy **firewalls, encryption, anti-malware, and intrusion detection systems.**
ii. Regularly back up data and test disaster recovery systems.
iii. Restrict system access to authorized users only.
iv. Conduct annual **cybersecurity audits and penetration tests.**
v. Train staff and members on **cybersecurity awareness** (e.g., phishing prevention).

### 7.7 Environmental, Social, and Governance (ESG) Risk Mitigation

i. Integrate **sustainability principles** into lending and investment policies.
ii. Promote environmentally friendly financing (e.g., renewable energy loans).
iii. Ensure gender inclusivity and diversity in governance structures.
iv. Adopt a **code of ethics** and enforce anti-corruption policies.
v. Report annually on ESG-related risks and achievements.

### 7.8 External Risk Mitigation

i. Monitor macroeconomic trends, inflation, and interest rate movements.
ii. Maintain political risk awareness and engage with sector regulators.
iii. Develop **scenario planning and stress testing** for shocks such as pandemics.
iv. Collaborate with cooperative federations and umbrella bodies to strengthen resilience.
v. Diversify income streams to reduce dependency on loan interest.

## 8. ROLES & RESPONSIBILITIES

Effective risk management requires clarity of roles and responsibilities across all governance organs, management, staff, and external stakeholders. At Energy RNWDT Sacco, responsibility for risk management is distributed as follows:

### 8.1 Board of Directors

i. Provide **strategic leadership and oversight** for the risk management framework.
ii. Approve the **Risk Management Policy** and ensure periodic reviews.
iii. Review and approve risk registers, reports, and mitigation strategies presented by management.

iv. Ensure the Sacco maintains adequate **capital, liquidity, and insurance cover** in line with regulatory requirements.
v. Oversee the development of a **Business Continuity and Disaster Recovery Plan.**
vi. Foster a risk-aware culture throughout the Sacco.

### 8.2 Supervisory Committee

i. Provide **independent oversight** of risk management processes.
ii. Review compliance with internal controls and statutory obligations.
iii. Audit the effectiveness of risk mitigation measures and report gaps to the AGM.
iv. Investigate risk incidents, member complaints, and governance breaches.

### 8.3 Credit Committee

i. Implement prudent **credit appraisal, approval, and monitoring** systems.
ii. Ensure compliance with **lending policies** to minimize credit risk.
iii. Monitor loan portfolio performance and recommend measures to address delinquency.
iv. Provide periodic credit risk reports to the Board and Supervisory Committee.

### 8.4 Management (CEO and Senior Managers)

i. Implement the Risk Management Policy on a day-to-day basis.
ii. Maintain and update the **Risk Register** for Board review.
iii. Develop and enforce internal control systems.
iv. Train staff on risk awareness and compliance obligations.
v. Report material risks promptly to the Board and regulators (SASRA).
vi. Ensure ICT, HR, procurement, and financial functions operate within risk frameworks.

### 8.5 Risk Management Committee (where established)

i. Provide specialized focus on risk oversight.
ii. Conduct **risk identification, assessment, and monitoring.**
iii. Recommend mitigation actions to management and the Board.
iv. Review emerging risks such as **cybersecurity, ESG, and market risks.**

### 8.6 Employees

i. Comply with Sacco policies, procedures, and internal controls.
ii. Report any irregularities, fraud, or potential risks to supervisors or through whistleblowing channels.
iii. Participate in risk awareness training.
iv. Safeguard Sacco resources, information, and assets entrusted to them.

### 8.7 Internal and External Auditors

i. **Internal Auditors:** Provide independent assurance on risk management processes, test internal controls, and recommend improvements.

ii. **External Auditors:** Assess whether risk management practices align with accounting, financial reporting, and regulatory standards.

### 8.8 Members

i. Provide accurate personal and financial information when joining and transacting with the Sacco.
ii. Honor loan obligations and adhere to Sacco bylaws.
iii. Actively participate in the AGM where risk matters are disclosed and discussed.
iv. Report unethical or risky practices through established complaint channels.

## 9. REPORTING & MONITORING

To ensure risks are effectively managed, Energy RNWDT Sacco shall maintain robust reporting and monitoring mechanisms that provide transparency, accountability, and early detection of emerging threats.

### 9.1 Risk Register

i. Management shall maintain a **comprehensive Risk Register** documenting all identified risks, their likelihood, impact, controls in place, and mitigation actions.
ii. The Risk Register shall be updated **quarterly** and reviewed by the Board of Directors.
iii. High-priority risks (rated "High" in the risk matrix) shall be escalated immediately to the Board Chairperson and CEO.

### 9.2 Reporting to the Board

i. Management shall submit **quarterly risk management reports** to the Board, covering:
    a. New risks identified during the quarter.
    b. Effectiveness of mitigation strategies.
    c. Status of unresolved or recurring risks.
    d. Compliance with SASRA prudential standards.
ii. The Board shall discuss and approve further mitigation or corrective measures as necessary.

### 9.3 Supervisory Committee Monitoring

i. The Supervisory Committee shall independently review the Sacco's risk management processes and provide reports to members during the AGM.
ii. The Committee shall verify that internal controls and governance practices are effectively enforced.

### 9.4 Internal & External Audit Reports

i. Internal Audit shall provide periodic reports on risk exposures and adequacy of internal controls.
ii. External Auditors shall include in their annual audit report an opinion on the Sacco's financial and operational risks.

### 9.5 Regulatory Reporting

i. The Sacco shall prepare and submit required risk-related reports to the **Sacco Societies Regulatory Authority (SASRA)** within the prescribed timelines.
ii. Reports shall include compliance with liquidity, capital adequacy, loan portfolio quality, and governance requirements.
iii. Any material risk incidents (e.g., fraud, liquidity crises, ICT breaches) shall be reported to SASRA immediately as per regulatory guidelines.

### 9.6 Member Reporting

i. Members shall be informed of the Sacco's risk exposures and mitigation strategies during the **Annual General Meeting (AGM)**.
ii. Key risk issues may also be communicated through newsletters, circulars, or digital platforms to enhance member awareness and trust.

### 9.7 Monitoring Tools

i. The Sacco shall use tools such as **risk dashboards, key risk indicators (KRIs), and compliance checklists** to continuously monitor the risk environment.
ii. Stress testing and scenario analysis shall be carried out periodically to test resilience against shocks such as economic downturns or liquidity stress.

## 10. NON-COMPLIANCE & SANCTIONS

Compliance with this Risk Management Policy is **mandatory** for all Board members, Committees, management, staff, and service providers engaged by Energy RNWDT Sacco. Any breach, negligence, or deliberate non-compliance shall be treated as a serious offense and addressed through appropriate disciplinary, regulatory, or legal action.

### 10.1 Internal Non-Compliance

i. **Board/Committee Members:**
   a. Failure to uphold fiduciary duty, concealment of risks, or negligence in oversight shall attract disciplinary measures, which may include suspension, removal from office, or being reported to SASRA for further action.

ii. **Management and Staff:**
   a. Breaches such as fraudulent activities, non-adherence to internal controls, or failure to report risks shall attract sanctions including warnings, suspension, termination, and recovery of losses.
   b. Staff implicated in fraudulent or reckless acts shall be reported to law enforcement authorities where criminal liability is established.

### 10.2 External Stakeholders

- Service providers, contractors, or consultants who breach risk-related contractual obligations (e.g., ICT security, data handling, audit standards) shall face sanctions including contract termination, blacklisting, and legal claims for damages.

### 10.3 Regulatory Non-Compliance

i. Any failure to comply with **SASRA prudential guidelines, the Co-operative Societies Act, POCAMLA[1], or the Data Protection Act** shall be treated as a major risk.
ii. The Sacco shall promptly report such breaches to regulators and cooperate with investigations.
iii. Penalties imposed by regulators due to negligence or misconduct shall be surcharged to responsible officers where applicable.

### 10.4 Corrective Actions

i. Non-compliance shall trigger immediate **root cause analysis** to prevent recurrence.
ii. The Sacco shall implement remedial measures such as staff retraining, process re-engineering, or system upgrades.
iii. Where losses occur due to negligence, responsible parties shall be held financially accountable in line with the law.

### 10.5 Whistleblower Protection

i. Staff, members, or stakeholders who report non-compliance or misconduct in good faith shall be **protected from retaliation.**
ii. Whistleblowing channels shall remain confidential and secure, encouraging a culture of openness and accountability.

## 11. REVIEW & APPROVAL

### 11.1 Policy Review Cycle

- This Risk Management Policy shall be **reviewed every three (3) years** or earlier if:
    - There are significant changes in **SASRA regulations, the Co-operative Societies Act, or national laws.**
    - The Sacco's operating environment changes materially (e.g., introduction of new products, technology upgrades, or regulatory directives).
    - Major risk incidents (such as fraud, liquidity crises, or cybersecurity breaches) expose gaps that require immediate revision.

### 11.2 Responsibility for Review

i. The **Board of Directors**, through the Risk Management Committee (or equivalent), shall coordinate policy reviews.

---

[1] **Proceeds of Crime and Anti-Money Laundering Act, 2009** of Kenya.

ii. The **Supervisory Committee** shall provide independent input on the adequacy and effectiveness of the policy.

iii. The **CEO and Management** shall propose amendments based on operational lessons, audit findings, and regulatory updates.

### 11.3 Approval

i. All amendments and reviews of this Policy must be approved by the **Board of Directors** and subsequently ratified by the **Annual General Meeting (AGM)**, in line with cooperative governance principles.

ii. Once approved, the revised Policy shall be communicated to **all staff, committees, and members** through official channels.

### 11.4 Record Keeping

The Sacco shall maintain an **archive of all previous versions** of this policy, along with Board and AGM resolutions approving each version, for regulatory inspection and governance accountability.

### 13.5 Effective Date

This policy shall come into effect on the date of its approval by the Board of Directors of Energy RNDT SACCO and shall remain in force until reviewed or replaced.

### 13.4 Approval of the Policy

We, the undersigned, individually and collectively, give commitment to the implementation of the Investment Policy by appending our signatures on behalf of the Board of Directors.

**Signed.**

Chairman:
Name ..... Paul N. Mbuthi ..... Sign ..... ..... Date... 8/11/2025

Secretary:
Name ..... Stella Ndumi ..... Sign ..... ..... Date.... 8/11/2025

Treasurer:
Name ..... Tom O. Olo O ..... Sign ..... ..... Date.....