ENERGY REGULATED NWDT SACCO SOCIETY LTD

DISASTER PREPAREDNESS AND BUSINESS CONTINUITY POLICY

September 2025

1.0 Policy Title and Purpose

This Disaster Preparedness and Business Continuity Policy (DPBCP) provides a framework to ensure that Energy Sacco remains resilient and continues to operate effectively in the event of disruptions caused by disasters, crises, or other emergencies.

The purpose of the policy is to:

- Protect members' funds, data, and trust.
- Safeguard the Sacco's staff, assets, and infrastructure.
- Ensure timely recovery of essential operations.
- Maintain compliance with regulatory requirements during and after disruptions.

2.0 Legal and Regulatory Framework

This policy is guided by:

- Co-operative Societies Act (Cap 490, Laws of Kenya).
- Sacco Societies Act (2008).
- SASRA Regulations, 2020 (Business Continuity and Risk Management).
- Data Protection Act (2019).
- Occupational Safety and Health Act (2007).
- The Sacco's by-laws, credit policy, and governance framework.

3.0 Scope

The policy applies to:

- All Sacco operations including **lending, savings mobilization, ICT systems, and member services**.
- All forms of disasters — natural (e.g., floods, drought, pandemics, earthquakes), technological (e.g., ICT system failure, cyberattacks), human-made (e.g., fraud, terrorism, fire), and operational (e.g., power outages, supply chain disruptions).
- All staff, elected officials, members, and service providers who play a role in Sacco continuity.

4.0 Disaster Preparedness Principles

The Sacco shall:

i. **Risk Assessment:** Regularly identify and evaluate potential threats to operations.
ii. **Prevention and Mitigation:** Put in place proactive measures to reduce disaster likelihood and impact.

iii. **Preparedness:** Develop response plans, train staff, and maintain emergency resources.
iv. **Response:** Ensure timely, coordinated, and effective actions during crises.
v. **Recovery:** Restore operations quickly while minimizing financial and reputational losses.
vi. **Resilience:** Build systems and culture that withstand future shocks.

5.0 Business Continuity Planning (BCP)

5.1 Critical Business Functions

The Sacco identifies the following as **critical functions** that must be sustained or restored immediately during disruptions:

- Member deposits and withdrawals.
- Loan disbursement and recovery.
- ICT systems (QFS platform, loan management system, accounting software).
- Communication with members and regulators.
- Financial reporting and compliance returns.

5.2 Continuity Strategies

- **ICT and Data Management:**
  - Daily backups of all digital records.
  - Offsite/cloud storage for critical data.
  - Alternative power supply (generators/UPS).
- **Human Resources:**
  - Cross-training of staff to perform essential roles.
  - Emergency staffing arrangements.
- **Physical Facilities:**
  - Fire safety systems and insurance coverage.
  - Secure physical records storage.
  - Alternate work sites or remote work arrangements.
- **Financial Resources:**
  - Maintenance of emergency funds.
  - Insurance coverage for assets, staff, and liabilities.
- **Member Services:**
  - Deployment of mobile and digital platforms for uninterrupted access.
  - Member helpdesk for crisis updates and support.

6.0 Disaster Response Protocol

- **Incident Reporting:** Any staff or member detecting a disaster must immediately notify the CEO.
- **Activation of Disaster Response Team (DRT):** The Board Chair, CEO, Treasurer, Secretary, ICT Officer, and Compliance Officer form the DRT.
- **Communication:** Only the Chair or CEO issues official communication to members, regulators, and the public.
- **Emergency Services:** Liaison with police, fire, medical, and disaster management authorities.
- **Regulatory Notification:** Mandatory notification to SASRA and other regulators in case of major disruption.

7.0 Roles and Responsibilities

- **Board of Directors:** Provide oversight, approve policies, and allocate resources.
- **CEO:** Overall responsibility for implementation and activation of business continuity plans.
- **Management Team:** Develop response procedures and train staff.
- **Staff:** Follow protocols, report incidents, and ensure safety of members and assets.
- **Supervisory Committee:** Independently review compliance and effectiveness of disaster preparedness measures.

8.0 Training and Awareness

- Staff and officials shall undergo **annual training** on disaster preparedness, ICT security, and emergency response.
- Regular **drills and simulations** shall be conducted to test readiness.
- Members shall be sensitized on how services will continue during emergencies.

9.0 Monitoring, Reporting, and Review

- Management shall prepare **quarterly reports** to the Board on disaster preparedness and continuity readiness.
- After each incident, a **post-disaster evaluation** shall be conducted, and lessons documented.
- This policy shall be **reviewed every three (3) years** or earlier as circumstances demand.

10.0 Effective Date and Adoption

This Disaster Preparedness and Business Continuity Policy takes effect upon approval by the Board of Directors and ratification by the AGM.

Signatories

Chairman:

Name: ..... Sign: ..... Date: .....

Secretary:

Name: ..... Sign: ..... Date: .....

Treasurer:

Name: TOM O OLO O Sign:  Date: .....

ANNEX 1: BUSINESS CONTINUITY PLAN (BCP)

A. CRITICAL BUSINESS FUNCTIONS CHECKLIST

The following functions are essential and must be prioritized in case of a disruption:

Function	Recovery Time Objective (RTO)	Responsible Officer	Backup/Alternative
Member deposits & withdrawals	Within 24 hours	Finance Manager	Mobile money/QFS system, partner bank
Loan disbursement & recovery	Within 48 hours	Credit Manager	Manual processing / emergency committee approval
ICT systems (QFS, loan management, accounting)	Within 12 hours	ICT Officer	Cloud backup, alternative server
Communication with members & regulators	Immediate (within 6 hours)	CEO / Board Chair	SMS, website, circulars, public notices
Financial & regulatory reporting	Within 72 hours	Finance Manager	Backup documentation & offsite records
Payroll & staff welfare	Within 72 hours	HR/Finance Manager	Partner bank arrangements

---

B. EMERGENCY RESPONSE PROTOCOL

1. **Incident Detection & Reporting**
    - Staff must immediately report disasters (fire, fraud, cyberattack, etc.) to the CEO.
    - An **Incident Report Form** must be completed within 24 hours.
2. **Activation of Disaster Response Team (DRT)**
    - CEO convenes the DRT (Board Chair, Treasurer, Secretary, ICT Officer, Compliance Officer).
    - Assess the situation and declare **Level of Crisis**:
        - *Level 1:* Minor (internal handling).

- *Level 2:* Moderate (Board involvement + member notification).
- *Level 3:* Major (regulator + public disclosure).

3. **Staff & Member Safety**
    - Evacuation procedures for physical threats (fire, natural disaster).
    - First aid support and liaison with emergency services.
4. **Crisis Communication**
    - Only the **CEO or Board Chair** issues external statements.
    - Members updated via SMS, website, and notices.
    - Regulators (SASRA, Commissioner for Co-operatives, FRC, KRA) notified as required by law.

C. ICT & DATA CONTINUITY

- **Data Backups:**
    - Daily backups stored in secure offsite/cloud storage.
    - Encrypted data transfers to prevent breaches.
- **System Recovery:**
    - Alternative server activated within 12 hours.
    - Manual loan/transaction registers maintained as fallback.
- **Cybersecurity Response:**
    - In case of breach, systems immediately isolated.
    - Incident reported to the **Office of the Data Protection Commissioner (ODPC)** within 72 hours as per the Data Protection Act (2019).

D. ALTERNATIVE OPERATIONS SITES

- Pre-identified **secondary office location** to be used if the main office is inaccessible.
- Remote working arrangements permitted for non-physical functions (loan processing, reporting, communication).

- Partner bank branches may be used for urgent member transactions.

E. FINANCIAL CONTINUITY

- Maintain an **Emergency Fund/Contingency Account** equivalent to at least **3 months of operating expenses.**
- Ensure adequate insurance coverage (fire, theft, fraud, cyber risk, staff cover).
- Activate overdraft or standby credit facility with partner bank if liquidity shortfall arises.

F. POST-DISASTER RECOVERY PROCESS

1. **Stabilization:** Restore essential operations within the defined RTOs.
2. **Damage Assessment:** Document financial, physical, ICT, and reputational impact.
3. **Regulatory Reporting:** Submit reports to SASRA and Commissioner for Co-operatives within statutory timelines.
4. **Member Engagement:** Update members on recovery progress and service resumption timelines.
5. **Debrief & Lessons Learned:** DRT to compile a post-disaster evaluation report for the Board and AGM.
6. **Policy Update:** Revise the BCP and Disaster Preparedness Policy based on lessons learned.

G. TRAINING & TESTING

- **Annual drills** (fire evacuation, data recovery simulations, crisis communication tests).
- **Staff induction training** on BCP protocols.
- **Periodic IT penetration testing** to evaluate system resilience.

H. REVIEW & APPROVAL

This BCP Annex shall be reviewed annually and updated as needed, with approval by the **Board of Directors** and ratification at the **AGM**.

ENERGY SACCO – BCP QUICK-RESPONSE CHECKLIST

In Case of Disaster or Emergency:

---

1. Detect & Report Immediately

- If you see/experience a **fire, fraud, cyberattack, system outage, or security threat**:
  - **Call/notify the CEO immediately.**
  - Fill out an **Incident Report Form** within 24 hours.

---

2. Safety First

- Evacuate staff and members if there is physical danger (fire, flood, earthquake).
- Provide first aid where needed.
- Call **999 / local emergency services** (fire, police, ambulance).

---

3. Activate Disaster Response Team (DRT)

- CEO convenes DRT (Board Chair, Treasurer, Secretary, ICT Officer, Compliance Officer).
- Assess level of crisis:
  - **Level 1:** Minor (handled internally).
  - **Level 2:** Moderate (Board + member notification).
  - **Level 3:** Major (regulator + public disclosure).

---

4. Communication Protocols

- **Only CEO or Board Chair** speaks to regulators, members, or media.
- Staff must not share unofficial information externally.
- Members will be updated via **SMS, website, office notices**.

---

5. ICT & Data Recovery

- ICT Officer activates **data backup & recovery plan**.
- Switch to alternative server/cloud storage if systems fail.
- Maintain **manual registers** for urgent transactions.

---

6. Member & Financial Continuity

- Ensure **deposits, withdrawals, and loan services** resume within 24–48 hours.
- Use **partner bank/QFS system** for emergency transactions.
- Access **emergency fund or overdraft facility** if liquidity shortfall arises.

---

7. Post-Disaster Recovery

- Stabilize essential operations first.
- Document damages and losses.
- Submit mandatory reports to **SASRA & Commissioner for Co-operatives**.
- Update members on progress.
- Conduct debrief & update BCP for future improvement.

⚠ **REMEMBER:**

- **Member funds & safety come first.**
- Always follow **chain of command**.
- Maintain **confidentiality & professionalism** at all times.

This **1-page summary** can be:

- Printed as a **wall poster** for Sacco offices.
- Shared as a **laminated pocket card** for staff.
- Distributed digitally via email or WhatsApp staff groups.

- Signed.
- Chairman:
- Name ..... Sign ..... Date.....
- Secretary:
- Name ..... Sign ..... Date.....
- Treasurer:
- Name ..... Sign ..... Date.....