JANUARY 1, 2025

refcom

RABAI EMPOWERMENT FOR COMMUNITY

Building passion for humanity through action to community

RECORD MANAGEMENT & INFORMATION COMMUNICATION TECHNOLOGY (ICT)

POLICY AND PROCEDRES

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Policy Abstract

In today's digital age, effective record management and the strategic use of information communication technology (ICT) are essential for the success of organizations like Rabai Empowerment for Community. This policy establishes a comprehensive framework for managing records in a manner that ensures accuracy, accessibility, and compliance with relevant legal and regulatory standards. Integrating ICT into record management practices in RefCom seeks to enhance operational efficiency, streamline processes, and enable informed decision-making. This approach not only supports the preservation of vital information but also promotes a culture of transparency and accountability within the organization.

The implementation of this policy will involve the adoption of modern technologies and systems that facilitate the secure storage, retrieval, and sharing of records. Training and capacity-building initiatives will be essential to equip staff with the necessary skills to utilize these tools effectively. Furthermore, the policy will outline procedures for data protection, ensuring that sensitive information is handled responsibly and in accordance with privacy regulations. Prioritizing record management and ICT, Rabai Empowerment for Community will be better positioned to achieve its mission, support its stakeholders, and respond proactively to challenges in the dynamic landscape of youth development and empowerment.

1.2 Purpose of the Policy

Securing a system for managing records and information technology in a work place is vital. RefCom also embraces this process to align itself with expected standards in an organization.

This policy ensures that RefCom's records and ICT systems are managed securely, efficiently, and in compliance with international standards. It aims to:

1. Protect sensitive information and prevent unauthorized access.
2. Ensure compliance with legal, regulatory, and ethical standards.
3. Establish a framework for efficient ICT use, cybersecurity, and data governance.

1.3 Scope and Applicability

The scope of the Record Management and Information Communication Technology (ICT) Policy for Rabai Empowerment for Community encompasses all aspects of how records are created, maintained, and utilized across the organization. This policy is applicable to all staff members, volunteers, and stakeholders involved in the collection, storage, retrieval, and dissemination of information. By establishing clear guidelines, the policy aims to ensure that all records, whether digital or physical are managed in a way that promotes efficiency, accountability, and compliance with legal and regulatory requirements. It also addresses the integration of ICT tools that enhance record management processes, thereby improving data accessibility and security.

Furthermore, the applicability of this policy extends to all programs and projects undertaken by the organization, ensuring that record management practices align with the organization's mission of empowering youth. The policy serves as a foundation for developing standardized procedures that foster consistency and reliability in record-keeping. Besides, it provides a framework for training and capacity-building initiatives, enabling staff to effectively utilize ICT resources in their daily operations. In doing so, the organization not only safeguards its valuable information but also enhances its ability to make data-driven decisions that further its goals in youth development and community engagement.

This policy applies to:

1. All employees, consultants, and third parties with access to RefCom's information systems.
2. All digital and physical records generated, received, or maintained by RefCom.
3. All ICT systems, including hardware, software, cloud storage, and communication tools.

1.4 Guiding Principles

RefCom Record management and ICT policy is aligned to international standards including but not limited to;

1. ISO 27001 (Information Security Management) – Ensures cybersecurity and data protection.
2. UN ICT Policy Framework – Defines global standards for technology and information management.
3. GDPR (General Data Protection Regulation) – Protects personal and organizational data privacy.
4. ISO 15489 (Records Management) – Provides guidelines for efficient record-keeping.
5. UN SDG 16 (Peace, Justice, and Strong Institutions) – Promotes transparency and accountability.

2. RECORD MANAGEMENT POLICY

2.1 Classification of Records

Classifying records in an organization is an important step in ensuring the usability, applicability and disposal mechanisms. Every organization is required to classify its records in accordance to their scope and depth. RefCom also classifies its records and information technology in its own unique way.

Records shall be categorized into:

1. Confidential Records – these include legal documents (constitution, policies, certificate of registration), employees' contracts and Personal Information Files (PIFs).
2. Internal Use Only Records – Records around this category include internal reports, emails and financial documents.
3. Public Records – These include published reports, press releases, promotional materials, newsletters.

2.2 Records Lifecycle Management

Records shall be managed in five phases:

1. Creation – This entails proper documentation of all records pertaining to RefCom in digital or physical form.
2. Storage – RefCom shall secure storage in various forms; either in cloud systems (ISO 27001 compliant) or physical archives and back-ups in a centralized machine that shall be accessed by specific personnel only.
3. Access and Use – Only authorized personnel may access records as per role-based access controls. Physical files shall be under lock and key, only accessible to the designated people, while soft copies stored in cloud system shall be given access to specific personnel.
4. Retention – Defined retention periods based on legal, regulatory, and operational needs.

5. Disposal – Secure destruction of outdated records following ISO 27001 and national data protection standards. Data management officers shall be allowed to sort all files that are outdated and dispose them in a secure manner.

2.3 Access, Security, and Confidentiality

Access, according to RefCom could be defined as the way records could be administered by specific people to encourage control and confidentiality.

Security may be referred to the safety of the records and information management within RefCom.

The degree of access, security and confidentiality is described below;

1. Employees shall only access records based on their roles and responsibilities. Physical files shall be stored in cabinets that have been provided access to specific personnel.
2. Digital records shall be protected by multi-factor authentication (MFA) and encryption.
3. Confidential records shall be stored in locked cabinets or secured digital folders. These will be limited to only the users of those files.

2.4 Records Retention and Disposal

Record retention in RefCom means the lifespan of the entire records within the organization. It ensures that the organization can utilize the records within a specific timeframe after which the record becomes non-usable.

Disposal according to RefCom refers to the process of discarding the same records in a secure manner to ensure that their do not fall into wrong hands.

RefCom records shall be retained and disposed as follows;

1. Financial and legal records: RefCom believes that these files can only be useful within a limited lifespan and shall be retained for 7 years.
2. Employee and HR records: This category of files shall be retained for 10 years' post-employment period after which they will be entitled for disposal.

3. Emails and general correspondence: RefCom will be allowed to synchronize its email and correspondences for a period of 3 years after which the emails shall automatically be disposed within the system.
4. Secure shredding and digital wiping shall be used for disposal. RefCom will be required to procure a paper shredder which will be used internally. During the disposal, the staff in line with the department shall be required to take part in the disposal process.

3. INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

Information and Communication Technology (ICT) plays a crucial role in shaping policy frameworks by enhancing access to information, improving communication efficiency, and facilitating data-driven decision-making. In the context of policy development, ICT tools enable the collection, analysis, and dissemination of information, which is essential for informed governance and stakeholder engagement. Furthermore, ICT fosters transparency and accountability by providing platforms for public participation and feedback, ultimately contributing to more effective and inclusive policy outcomes. As such, integrating ICT into policy processes is vital for promoting innovation and addressing contemporary challenges in various sectors.

3.1 ICT Governance and Compliance

1. All ICT systems must comply with ISO 27001 and national accepted standards.
2. Employees must use organizational devices, networks, and systems responsibly.
3. Software and applications must be licensed and approved by the IT Department.

3.2 Cybersecurity and Data Protection

1. Firewalls, antivirus software, and intrusion detection systems must be implemented.
2. Regular cybersecurity training shall be conducted for employees.
3. Passwords must be updated every 90 days and follow strict complexity guidelines.
4. Personal data shall be encrypted and stored in compliance with GDPR.
5. Remote access shall be secured via VPNs and multi-factor authentication (MFA).

3.3 ICT Infrastructure and Asset Management

1. All ICT assets (laptops, servers, mobile devices) must be registered.
2. Employees are responsible for the safekeeping of assigned devices.
3. ICT equipment that is obsolete must be disposed of following environmental regulations.

3.4 Digital Communication and Social Media Use

1. Official email accounts must be used for work-related communication.
2. Employees must not share sensitive information via personal emails or social media.
3. Official social media pages must be managed by authorized personnel.

4. ROLES AND RESPONSIBILITIES

In the formulation and implementation of effective policies, clearly defined roles and responsibilities are essential to ensure accountability, streamline operations, and facilitate collaboration among stakeholders.

This section outlines the specific duties and obligations of various actors involved in the policy process.

Delineating these roles, the policy aims to foster a cohesive approach to achieving shared goals, enhance transparency in execution, and promote a culture of responsibility that is vital for the successful delivery of policy outcomes.

4.1 Record Management Officers

1. Oversee storage, classification, and disposal of records.
2. Ensure compliance with ISO 15489 (Records Management Standard).

4.2 ICT and Cybersecurity Team

1. Implement cybersecurity policies and manage IT infrastructure.
2. Conduct regular security audits and risk assessments.

4.3 Employee Responsibilities

1. Follow record management and ICT policies.
2. Report any data breaches, unauthorized access, or ICT failures immediately.

5. MONITORING, EVALUATION, AND POLICY REVIEW

Monitoring, evaluation, and policy review are integral components of the policy development process, ensuring that policies are effectively implemented and continuously improved. This section emphasizes the importance of establishing robust monitoring and evaluation frameworks that provide systematic feedback on policy performance, outcomes, and impacts.

Assessing the effectiveness of policies regularly against established objectives, stakeholders can identify successes, address shortcomings, and make informed adjustments.

Additionally, conducting periodic policy reviews promotes a culture of accountability and transparency, enabling policymakers to respond to emerging challenges and evolving societal needs, ultimately enhancing the relevance and sustainability of policy initiatives. Steps include;

1. Annual audits shall assess compliance with ICT and record management standards.
2. Employee feedback shall be collected biannually to improve policy effectiveness.
3. This policy shall be reviewed every three years or as required.

6. COMPLIANCE AND ENFORCEMENT

Compliance and enforcement are critical elements in the formulation of effective policies, as they ensure that established regulations and standards are adhered to by all stakeholders. This section highlights the necessity of creating a robust framework for monitoring compliance, which involves not only the implementation of policies but also the mechanisms for reporting, assessing, and enforcing adherence. By clearly defining roles and expectations, policies can foster a culture of accountability and promote adherence to legal and ethical standards. Furthermore, effective enforcement strategies are essential for addressing non-compliance, thereby safeguarding the integrity of the policy objectives and ensuring that intended outcomes are achieved.

1. Violations of this policy shall result in disciplinary action, including termination.
2. Legal action may be taken in case of intentional misuse or data breaches.
3. Employees shall sign a compliance agreement upon joining the organization.

7. APPROVAL AND IMPLEMENTATION

In the context of policy formulation, the approval and implementation phases are crucial for the effective operationalization of guidelines pertaining to record management and information communication technology (ICT). In RefCom, the approval process will involve the thorough evaluation of proposed policies to ensure they align with organizational goals and legal requirements.

This will pave way to the implementation phase, requiring a strategic approach to roll out the new directives internally. RefCom will need to train its personnel, allocating resources, and establishing procedures that integrate record management practices with ICT systems, ensuring that all relevant information is accurately captured, stored, and accessible.

Effective implementation is further supported by the integration of technology in record management, which enhances efficiency and accuracy in handling information. Policies must stipulate clear responsibilities for staff involved in record management and the use of ICT, ensuring everyone understands their roles in maintaining compliance.

Besides, RefCom will provide ongoing support and resources to facilitate smooth implementation, including regular training and updates on technological advancements. This proactive approach not only ensures adherence to established policies but also promotes a culture of accountability and continuous improvement within RefCom.

Aligning record management and ICT strategies with policy objectives enhances their operational efficiency and responsiveness to emerging challenges in information governance.

This policy is approved by the Board of Directors of RefCom and shall take effect immediately.

"*…………I am proud to endorse this Record management and Information Communication and Technology Policy as a cornerstone of our commitment to promoting a multifaceted approach in managing information at our workplace. This manual provides clear guidance on all aspects of managing records, information and technology, ensuring consistency, transparency, and compliance in communication. It reflects our dedication to provide a clear pathway while contributing to our strategic goals. I call upon all staff and stakeholders to embrace the principles outlined herein as we work together to achieve our mission and create a positive, collaborative environment.………..."* **Chief Program Officer (CPO)**

This policy is effective as of 5th January 2025 and will remain in force until further notice.

Approved by:

S/NO	Names, Postal Addresses, position held and Occupations of Directors	ID number of Director	Mobile Number of Director	Signatures of Directors
1.	**James Katana Gibson**	**21005098**	**0723 734 303**	
2.	**Edward Chongwa Gamimbah**	**14499314**	**0721 786 550**	
3.	**Lennox Ringa Mwabaya**	**28186907**	**0718 056 796**	
4.	**Alicia Wanjoru Pauline**	**35195779**	**0796 981 760**	
5.	**Douglas Shauri Saha**	**11876086**	**0711 449 317**	