



Marsabit Water and Sewerage Company (MARWACO)

ICT Policy and Procedures Manual

*Leveraging technology for effective
water and wastewater management*

October 2025

Preface

The Marsabit Water and Sewerage Company Limited (MARWASCO) recognizes Information and Communication Technology (ICT) as a cornerstone of modern utility management. As the company expands its mandate to deliver reliable, inclusive, and sustainable water and sanitation services across Marsabit County, the need for a structured, secure, and forward-looking ICT framework has become paramount.

This ICT Policy and Procedures Manual provide a comprehensive guide for the acquisition, use, governance, and protection of digital systems and resources within MARWASCO. It aligns with Kenya's national legislation—including the Data Protection Act, Water Act, and Public Finance Management Act—and integrates sectoral best practices to ensure compliance, transparency, and operational resilience.

The policy reflects MARWASCO's commitment to digital transformation, institutional accountability, and service excellence. It outlines clear standards for equipment procurement, software acquisition, data management, staff training, and cybersecurity, while promoting responsible use and continuous improvement across all departments.

Developed through a participatory process and validated with support from PACIDA, this policy is a living document that will evolve with technological advancements, regulatory shifts, and stakeholder needs. It serves as both a strategic roadmap and an operational tool to guide MARWASCO's journey toward a digitally empowered future.

Joseph G Halakhe



Chairman

Board of Directors

Marsabit Water and Sewerage Company Limited (MARWASCO)

Foreword

As the Managing Director of Marsabit Water and Sewerage Company Limited (MARWASCO), I am pleased to present this ICT Policy and Procedures Manual, a critical milestone in our journey toward digital transformation and operational excellence.

This policy reflects MARWASCO's strategic commitment to harnessing Information and Communication Technology (ICT) to improve service delivery, enhance data security, and promote institutional accountability. It aligns with Kenya's national legislation—including the Data Protection Act, Water Act, and Public Finance Management Act—and integrates sectoral best practices to ensure compliance, resilience, and sustainability.

The development of this policy was informed by a participatory process involving MARWASCO staff, management, and Board of Directors, with generous support from PACIDA. Their insights and technical contributions have ensured that the policy is both practical and forward-looking, tailored to the unique needs of our operational environment.

I urge all staff, contractors, and stakeholders to familiarize themselves with the provisions of this policy and uphold its principles in their daily work. Together, we can build a digitally empowered utility that delivers dependable, inclusive, and customer-centered water and sanitation services across Marsabit County.

Stephen Sora



Managing Director

Marsabit Water and Sewerage Company Limited (MARWASCO)

Date: 1st October 2025

Acknowledgement

We extend our sincere appreciation to PACIDA for generously funding the development and validation of this Information, Communication, and Technology (ICT) Policy and Procedures Manual. PACIDA's support has been instrumental in strengthening MARWASCO's commitment to digital transformation, governance, and operational efficiency.

We also acknowledge the dedication and collaborative efforts of MARWASCO's staff and management and the Board, whose insights and technical contributions shaped the content and relevance of this policy. Their commitment to institutional growth and delivery of service is commendable.

Finally, we thank the MARWASCO Board of Directors (BOD) for the strategic overseeing role and formal approval of this policy. The Board's leadership ensures that our ICT practices align with organizational strategic goals and national compliance standards.

Acronyms/Abbreviations

ATMs	-	Automated Teller Machines
AUTOCAD	-	Automated Computer Aided Design
COK	-	Constitution of Kenya
DPO	-	Data Protection Officer
ERP	-	Enterprise Resource Planning
GEA	-	Government Enterprise Architecture
GIS	-	Geographic Information System
HEC – RAS	-	Hydrologic Engineering Center – River Analysis System
HR	-	Human Resources
IAM	-	Identity and Access Management
ICT	-	Information Communication and Technology
ID	-	Identity Card
IoT	-	Internet of Things
IP	-	Internet Protocol
KENIC	-	Kenya Network Information Centre
MARWASCO	-	Marsabit Water and Sewerage Company Limited
MDAC	-	Ministries, Departments, Agencies, and Counties
NEMA	-	National Environment Management Authority
PFMA	-	Public Finance Management Act
PPADA	-	Public Procurement and Disposal Act
QGIS	-	Quantum Geographic Information System
QR	-	Quick Response
RFID	-	Radio Frequency Identification

ROHS	-	Restriction of Hazardous Substances
SaaS	-	Subscription based Licensing.
SCADA	-	Supervisory Control and Data Acquisition
SEO	-	Search Engine Optimization
SLA	-	Service Level Agreement
SOPs	-	Standard Operating Procedures
SRC	-	Salaries and Remuneration Commission
SSL	-	Secure Sockets Layer
SWAT	-	Soil and Water Testing Tool
TCO	-	Total Cost of Ownership
TLS	-	Transport Layer Security
WASREB	-	Water Services and Regulatory Board

Table of contents

Table of Contents

Preface	i
Foreword	ii
Acknowledgement	iii
Acronyms/Abbreviations	iv
Table of contents	vi
ICT Policy Statement	ix
EFFECTIVE DATE	x
1. Background	1
2. Introduction	1
2.1. Purpose	2
2.2. Objectives	2
2.3. Scope	2
2.4. Review and Compliance	2
3. Alignment of MARWASCO ICT policy with National Legislation	2
3.1. The Water Act 2016 (Cap.372) and Water (Services) Regulations, 2025.	3
3.2. Guidelines on Management of ICT Resources in MDACs(2024).....	3
3.3. Data Protection Act, 2019.	3
3.4. Public Finance Management Act, 2012.....	3
3.5. Kenya National ICT policy (2020).....	3
3.6. Access to information Act, 2016.	3
3.6.1. Right to Information.	4
3.6.2. Proactive Disclosure	4
3.6.3. Designation of Information Officers.....	4
3.6.4. Application Process	4
3.6.5. Grounds for Refusal.	4
3.6.6. Protection for Whistleblowers, offences, and penalties.	5
4. Webhosting, Email Communication, and role of third parties in hosting	5
4.1. Email Communication.....	5
4.2. Company Domain and Webhosting.....	5

4.3.	Role of third party in webhosting and safeguards for MARWASCO	6
1.	Data Security & Privacy.....	6
2.	Access Control & Credential Management	6
3.	Backup & Disaster Recovery	6
4.	Uptime & Incident Response	6
5.	Compliance & Audit Rights	7
6.	Termination & Data Portability	7
4.4.	Mitigation of cybersecurity threats.....	7
4.5.	Antivirus procurement and protection of MARWASCO ICT assets	7
4.6.	Use of Open-Source Software.....	7
5.	Acquisition and usage of ICT Equipment and Software	8
5.1.	Standardization and specifications for equipment purchase.....	8
5.2.	ICT Asset tagging and tracking procedures.	9
5.3.	Best practices in software acquisition for MARWASCO.....	10
5.4.	Options for software acquisition by MARWASCO.....	11
5.5.	Acceptable ICT Equipment and Software use practices.....	12
5.6.	Non - acceptable practices Use of ICT Equipment and Software.....	12
5.	Data Management and Security	13
5.1.	Legal obligation to protect personal data.....	13
5.2.	Mandatory data governance structures	13
5.3.	Customers and transparency.....	14
5.4.	Breach notification and accountability	14
5.5.	Cybersecurity and system design.....	14
5.6.	Data minimization and retention.....	14
6.	Cybersecurity and Data Protection	15
6.1	Overview	15
6.2	Governance and Accountability	15
6.3	Data Protection and Privacy	15
6.4	System and Network Security	15
6.5	Incident Response and Recovery.....	15
6.6	User Awareness and Training.....	15

6.7 Third-Party and Vendor Compliance	16
6.8 Monitoring, Audit, and Continuous Improvement.....	16
7. Hardware and Software Management	16
8. Incident Reporting	16
9. Training and Awareness	17
10. Implementation and Compliance with the ICT policy	17
11. Monitoring and Review.....	17
Annexes	18
Annex 1: MARWASCO ACCESS TO INFORMATION REQUEST FORM	18
Annex 2: Access to Information Compliance Checklist for MARWASCO	20
Annex 3: Decision Matrix for Software ownership Models	21
Annex 4: Asset Register Template.....	0

ICT Policy Statement

MARWASCO is committed to leveraging Information and Communication Technology (ICT) as a strategic driver of operational efficiency, service delivery, and data security in the water and sanitation sector. This policy establishes a guiding framework to ensure that ICT systems are deployed and managed in a manner that supports the company's mission of delivering reliable, inclusive, and sustainable services to the communities of Marsabit County.

The objectives of this policy are to ensure secure and reliable ICT systems that underpin core business functions, promote responsible use of digital tools, safeguard sensitive data, and maintain compliance with national legislation such as the Data Protection Act. It also seeks to foster digital literacy among staff and align ICT investments with MARWASCO's long-term goals for innovation, resilience, and customer satisfaction.

This policy applies to all employees, contractors, and stakeholders who interact with MARWASCO's ICT infrastructure, systems, and data. It defines acceptable use, clarifies responsibilities, and promotes a culture of accountability and continuous improvement. All users are expected to uphold cybersecurity standards, respect data privacy, and contribute to the efficient use of ICT resources.

Policy guidelines include implementing robust cybersecurity protocols, optimizing ICT assets to reduce costs, providing regular training for users, and ensuring timely system upgrades and backups. MARWASCO will monitor ICT performance, adapt to emerging technologies, and maintain systems that support billing, HR, inventory, and GIS-based asset tracking. Technology alignment with organizational goals will be prioritized to ensure scalability and sustainability.

This policy shall be reviewed annually to remain responsive to technological advancements and regulatory changes. Non-compliance may result in disciplinary action in accordance with company procedures. Oversight will be provided by MARWASCO's ICT Committee, which will ensure implementation, recommend strategic upgrades, and uphold standards that reflect the company's commitment to secure, efficient, and community-centered service delivery.

EFFECTIVE DATE

This policy is approved by the MARWASCO's Board of Directors for implementation effective 1st October 2025.

On behalf of the Board

Joseph G Halake



Chairperson

MARWASCO

Stephen Sora



Managing Director

MARWASCO

1. Background

Marsabit Water and Sewerage Company Limited (MARWASCO) is a county-owned water utility company tasked with delivering reliable water supply and sanitation services to residents across Marsabit County. As demands for effective and sustainable service delivery increase and stakeholders' expectations evolve, technology has become central to MARWASCO's mandate of ensuring operational efficiency, transparency, and customer satisfaction.

Recognizing the transformative role of Information and Communication and Technology (ICT) in water and sanitation utility management, MARWASCO has developed this ICT policy and procedures manual to guide digital systems adoption, integration, infrastructure development, data governance, and improved cybersecurity environment within the company. The policy aligns with key national ICT policy and strategic frameworks—including Kenya's Digital Economy Blueprint, Vision 2030, and Water Sector Strategic Plan—and adheres to guidelines set out by Water Services Regulatory Board (WASREB) and the Salaries and Remuneration Commission (SRC).

The increasing use of ICT across MARWASCO's operational domains—billing, customer service, Geographical Information System (GIS) mapping, asset management, finance and commercial integration using Enterprise Resource Planning (ERP) and internal communication—underscores the need for a structured approach to system security, staff training, technology procurement, and change management.

Moreover, the integration of ICT will support performance-based contracting, promote real-time data collection, and enhance service delivery, especially in remote and hardship-prone areas. This policy provides a framework for managing ICT systems and resources, safeguarding digital assets, supporting innovation, and building digital capacity across MARWASCO's departments. It will serve as a living document that evolves with technological trends, regulatory requirements, and user needs.

The objectives of MARWASCO's ICT policy are to provide structure, security, and efficiency in the management of information and communication technology resources.

2. Introduction

The Marsabit Water and Sewerage Company Limited (MARWASCO) recognizes the transformative power of Information and Communication Technology (ICT) in delivering dependable, efficient, and customer-focused water and sanitation services. As the demand for sustainable water utility company management grows, ICT has become an essential pillar in enhancing operational transparency, data-driven decision-making, and stakeholder engagement.

This ICT policy provides a structured framework to guide the acquisition, use, security, and maintenance of digital systems and infrastructure across MARWASCO. It aligns with national ICT standards, regulatory requirements, and the company's strategic objectives

to ensure that technology serves as a catalyst for innovation, accountability, and continuous improvement.

By adopting this policy, MARWASCO commits to fostering a digitally empowered workforce, safeguarding sensitive information, and leveraging ICT to improve service delivery and operational resilience.

2.1. Purpose

The purpose of this policy is to establish a strategic framework for the acquisition, use and management of MARWASCO's Information, Communication and Technology (ICT) resources to enhance operational efficiency, service delivery, and data security within the company.

Our aim is to ensure secure, efficient, and sustainable use of ICT resources within MARWASCO, supporting the delivery of reliable water and sanitation services to the community and its stakeholders.

2.2. Objectives

- i. Ensure secure and reliable ICT systems that support company's core business functions.
- ii. Promote responsible use of digital tools and resources.
- iii. Safeguard sensitive data and maintain compliance with relevant regulations.
- iv. Foster digital literacy and continuous improvement among staff.
- v. Align ICT investments with organizational strategic goals for growth and sustainability.

2.3. Scope

This policy applies to all MARWASCO employees, contractors, stakeholders, and third-party vendors who access or manage the company's ICT resources (Infrastructure and data) within the organization.

2.4. Review and Compliance

This policy shall be reviewed annually to remain responsive to technological advancements and regulatory changes.

Non-compliance by staff with the policy guidelines may result in disciplinary action in accordance with company's Human Resources Policy and Procedures Manual.

3. Alignment of MARWASCO ICT policy with National Legislation

MARWASCO's ICT Policy is designed to operate within Kenya's broader legal and regulatory environment, ensuring compliance, accountability, and strategic alignment with national priorities. By aligning with these national frameworks, MARWASCO's ICT Policy ensures legal compliance and institutional credibility; strategic use of technology

to improve water service delivery; protection of citizen data and digital rights and contribution to Kenya's digital transformation agenda.

3.1. The Water Act 2016 (Cap.372) and Water (Services) Regulations, 2025.

These regulations govern the licensing, service standards, and operational accountability of water service providers in Kenya. MARWASCO's use of digital platforms for billing, customer feedback, and operational monitoring directly supports the regulatory emphasis on transparency, efficiency, and service quality.

3.2. Guidelines on Management of ICT Resources in MDACs (2024)¹.

These guidelines are issued by the Ministry of Information, Communications and the Digital Economy and provide a national framework for ICT governance in Ministries, Departments, Agencies, and Counties. MARWASCO's policy mirrors the guidelines on ICT strategy development, infrastructure management, cybersecurity, and digital innovation.

The ICT policy supports the adoption of Government Enterprise Architecture (GEA), promoting interoperability and standardization across public sector ICT systems.

3.3. Data Protection Act, 2019.

This act governs the collection, processing, storage, and sharing of personal data in Kenya. In line with this Act, MARWASCO's policy includes provisions for data privacy, secure handling of customer information, and staff training on data protection—ensuring full compliance with the law.

3.4. Public Finance Management Act, 2012

This act mandates prudent use of public resources and in furthering the goals of the Act, MARWASCO's ICT policy promotes cost-effective procurement, lifecycle management of ICT assets, and digital accountability mechanisms.

3.5. Kenya National ICT policy (2020)

This policy outlines the government's vision for ICT as a driver of economic growth and public service transformation. MARWASCO's digital initiatives—such as e-billing, GIS mapping, and mobile service platforms—support the national goals of digital inclusion, innovation, and e-governance.

3.6. Access to information Act, 2016.

Kenya's framework for freedom of information access is anchored in Article 35 of the Constitution and operationalized through the Access to Information Act, 2016.

¹ [ICT Resource Guidelines – Ministry of ICT](#)

Together, they guarantee citizens the right to access information held by public entities and certain private organizations.

MARWASCO will embrace the principles outlined in the law relating to access to information to promote transparency and accountability, enhance structured record-keeping and disclosure mechanisms and encourage citizen engagement and trust.

3.6.1. Right to Information.

In line with the Constitution of Kenya 2010 (COK 2010), article 35, every citizen has the right to access information held by the State or by another person required for the exercise or protection of any right or fundamental freedom. Within this context, citizens can request information from public entities and private bodies performing public functions.

MARWASCO will comply with these constitutional requirements and ensure that valid requests are responded to within 21 days, or 48 hours if the information is needed to safeguard life or liberty.

3.6.2. Proactive Disclosure

To facilitate access to information of public interest, MARWASCO will proactively publish relevant information including assessment reports, budgets, policies, and service delivery data.

3.6.3. Designation of Information Officers.

At its discretion, MARWASCO will appoint or designate internal Information Access Officer(s) to manage requests and ensure compliance.

3.6.4. Application Process

Any information requests to MARWASCO must be made in writing, stating the information sought, beneficiary of the information and the reason for the request (if applicable). This requester will complete the Information Access request form in Appendix 2.

MARWASCO may charge fees for information that may require reproduction but not for access itself.

3.6.5. Grounds for Refusal.

Access to information requests may be denied on the following grounds:

- It compromises national security or public safety.
- It infringes on the privacy of individuals.
- It relates to ongoing investigations or legal proceedings.
- It violates intellectual property rights of the service provider.

3.6.6. Protection for Whistleblowers, offences, and penalties.

Individuals who disclose information in good faith will be protected from retaliation internally.

Any staff member or person who alters, defaces, or destroys information unlawfully will face disciplinary procedures (if internal) and may face legal proceedings as per the law.

4. Webhosting, Email Communication, and role of third parties in hosting

4.1. Email Communication

MARWASCO is committed to maintain an identifiable and consistent company brand, in line with MARWASCO's strategic objective on branding and brand identity.

- i. To fulfill this commitment, all MARWASCO staff, management, and board members will use company email address and social media handles for official communication.
- ii. ICT Department will establish email addresses for all staff members and leadership team and configure emails for offline and remote access to allow those working away from office to use official communication channels.
- iii. ICT Department will maintain a database of log-in credentials and personnel are discouraged from sharing individual log-in detail with non-authorized persons.
- iv. Access to company information will be regulated via user authentication with privileges set according to relevance of information required for the staff's execution of their roles.
- v. Access to and sharing sensitive data through email will require prior authorization by relevant managers.

4.2. Company Domain and Webhosting

- a. As a commercial entity, MARWASCO will adopt for its use a [.co.ke](#) domain for commercial entities.
- b. Domain registration and hosting service will be provided through service providers accredited by the Kenya Network Information Centre (KENIC).
- c. Preference will be given to ICT service providers with hosting infrastructure located within Kenya for faster access speeds and better SEO for local audiences.
- d. The registration and hosting services will be sourced and procured in line with the Procurement Policy and Procedures Manual and governed by a service level agreement (SLA) that is legally enforceable in case of breach of contract.
- e. As a minimum the hosting service provider will provide a package that includes Control panel access (e.g., cPanel), branded email services (e.g., info@marwasco.co.ke), DNS management and security features including spam filters and SSL certification.

- f. ICT Department will regularly review and update the minimum specifications for providers hosting the company domain and website to guarantee security of data, efficiency in service provision and maintain an up-time of at least 99.9%, as per industry standards.

4.3. Role of third party in webhosting and safeguards for MARWASCO

To safeguard MARWASCO's data and systems where third-party entities are hired to host company domain and website, a clear service agreement will be entered into with the selected provider with clear, enforceable conditions that reflect best practices in cybersecurity, data governance, and legal compliance covering key areas including:

1. Data Security & Privacy

- i. Hosting provider must comply with the Kenya Data Protection Act and implement industry-standard encryption (SSL/TLS).
- ii. All customer and operational data must be stored securely, with access restricted to authorized personnel only.
- iii. Provider must not share, sell, or repurpose MARWASCO's data without written consent.

2. Access Control & Credential Management

- a. MARWASCO retains full administrative control over domain, hosting panels, and email accounts.
- b. Provider must enforce strong password policies and offer two-factor authentication (2FA) for control panel access.
- c. Login credentials must be handed over securely and updated upon staff transitions.

3. Backup & Disaster Recovery

- Daily or weekly automated backups must be included, stored offsite or on redundant servers.
- The provider must commit to a defined data recovery time in case of system failure or breach.
- Backup logs and restoration procedures should be accessible to MARWASCO's ICT team.

4. Uptime & Incident Response

- a) Minimum 99.9% uptime guarantee, excluding scheduled maintenance (with 24-hour notice).
- b) Provider must offer 24/7 monitoring and respond to security incidents within a defined SLA requirement (e.g., 30 minutes).
- c) All breaches or attempted intrusions must be reported to MARWASCO within 12 hours, including actions taken to avert data loss.

5. Compliance & Audit Rights

- ✓ Hosting infrastructure must meet ISO 27001 or equivalent security standards.
- ✓ MARWASCO reserves the right to conduct periodic security audits or request audit reports.
- ✓ Provider must cooperate with any regulatory investigations or compliance checks within specified time limits.

6. Termination & Data Portability

- I. Upon termination, provider must ensure full data export in usable formats (e.g., SQL, CSV, HTML).
- II. The service provider must permanently delete all MARWASCO data from its servers within 30 days.
- III. Domain ownership must remain with MARWASCO throughout and after the contract period.

4.4. Mitigation of cybersecurity threats

MARWASCO like other water utility companies in Kenya, increasingly recognize the importance of cybersecurity, antivirus protection, and open-source software as part of their digital transformation and resilience strategies.

Vulnerability to cyber threats range from ransomware and phishing to attacks on SCADA and billing systems. MARWASCO will mitigate this risk through:

- Adopting Identity and Access Management (IAM) to control user access across IT and operational systems. IAM frameworks will define roles, enforce secure logins, and automate permissions.
- Conducting risk assessments, implementing firewalls, and training staff on cybersecurity awareness.
- Integrating remote monitoring and Internet of Things (IoT) based leak detection, which requires secure data transmission protocols.
- Developing and implementing incident response plans and conducting regular audits, to guarantee security of digital billing and customer data.

4.5. Antivirus procurement and protection of MARWASCO ICT assets

MARWASCO will prioritize procuring corporate-grade antivirus solutions through formal tender processes as per the Procurement Policy and Procedures Manual. The tenders shall include clauses on license validity, centralized management, multi-layered approach to digital protection and integration with existing systems.

4.6. Use of Open-Source Software

Use of Open-Source Software and tools: The open-source tools may be used due to their affordability, flexibility, and transparency.

Platforms like QGIS for GIS mapping, HEC-RAS for river modeling, and SWAT for watershed analysis; ubuntu-based systems are available and are currently used to power smart water ATMs and digital meters in underserved counties, enabling mobile payments and real-time monitoring.

The open-source software supports custom dashboards, leak detection, and billing systems, as an alternative to expensive proprietary licenses but they need to be paired with secure configurations and local capacity building.

5. Acquisition and usage of ICT Equipment and Software

MARWASCO considers procurement of ICT equipment as a long-term investment that will enable the company to gain value, reliability, and strategic fit. To decide on the choice of suppliers, the company will consider business needs alignment where equipment will be matched to actual operational needs and future scalability; compatibility so that new equipment can integrate smoothly with existing systems, software, and networks and total cost of ownership, to forecast beyond purchase price and consider other costs related to maintenance, energy consumption, support, and upgrade cost

As a matter of policy, the company will prioritize procurement of ICT equipment from branded manufacturers / suppliers to guarantee product authenticity, after sales services, maximize reliability, warranty support, certification and standardization, security and legal compliance.

5.1. Standardization and specifications for equipment purchase

- a. All MARWASCO ICT equipment will be procured from certified dealers and authorized distributors who can guarantee product authenticity, offer after sales services via service level agreements (SLAs), provide easier and faster warranty claims, meets industry and donor standards and have capacity for bulk supply and financing. CT Manager and which.
- b. The ICT department will ensure that the procurement of ICT equipment complies with Restriction of Hazardous Substances (RoHS) standards and balance's technical reliability, cost-effectiveness, and regulatory compliance.
- c. ICT purchases will be aligned with MARWASCO's strategic plan, digital transformation strategic goals, and donor requirements, where appropriate.
- d. ICT Department will develop standardized technical specifications for common equipment (e.g., laptops, printers, servers) and prioritize interoperability with existing and future systems (e.g., ERP, SCADA, GIS, AUTOCAD). A sample checklist for common equipment is presented in Table 1.
- e. In developing the technical specifications, the Department will refer to good practices including reference to national ICT guidelines from ICT Authority Kenya and sector specific Standard Operating Procedures (SOPs).

- f. All ICT equipment will be RoHS compliant, from branded manufacturers, supplied through certified and authorized dealers with take-back programs, extended warranties, and local servicing.
- g. The Department shall ensure that all ICT purchases support secure data handling, especially for customer and financial systems, encryption-ready devices with access control features, and compliance with Kenya's Data Protection Act.
- h. As a matter of best practice, ICT department will adopt the Lifecycle Costing approach and evaluate total cost of ownership including purchase price + maintenance + energy + disposal to avoid low-cost options that result in high long-term costs due to frequent breakdowns or incompatibility.
- i. Consideration will be given to modular, energy efficient, durable, repairable, and recyclable equipment to reduce e-waste in line with NEMA's e-waste management policies and guidelines.

Table 1: Sample checklist with key considerations for common ICT equipment.

Item	Considerations
Laptops & Desktops	RAM ≥ 8GB, SSD storage, rugged casing
Printers & Scanners	Duplex printing, toner efficiency
Servers & Networking Gear	Redundancy, backup power, secure access
GIS & SCADA Equipment	Compatibility with existing platforms
Software Licenses	Legal compliance, scalability, cloud-readiness
Accessories	Surge protectors, UPS, dust-proof enclosures

5.2. ICT Asset tagging and tracking procedures.

- i. Each ICT item (e.g., laptops, routers, servers) will be identified, labelled, and assigned to a unique asset ID. A physical tag, typically a barcode, QR code, or RFID label will be affixed to the equipment for easy tracking.
- ii. Asset details such as serial numbers, model, location, assigned user, purchase date, and warranty status will be recorded in an asset management system, inventory database or asset register (Annex 4) that will be kept by ICT Department.
- iii. Regularly – (at least once per quarter) tagged assets will be scanned and updated to reflect changes in location, status, or ownership to support audits, maintenance schedules, and lifecycle management.
- iv. Asset tracking will ensure security of company assets and tagging ensures accountability, prevents loss or theft, and supports compliance with IT policy and financial reporting standards.

5.3. Best practices in software acquisition for MARWASCO

- i. ICT department will identify user needs through participatory needs assessments with all departments considering company's strategic growth goals and demands for compliance with regulatory requirements.
- ii. The company will prioritize modules that support asset management, billing, GIS integration, workflow management, Computer Aided Design (CAD) for technical services and regulatory compliance.
- iii. The chosen platforms must provide interoperability and easily integrate with existing systems for HR, finance, GIS, and early warning dashboards and ensure compatibility with mobile devices for field data collection and real-time updates.
- iv. As a growing company, MARWASCO will opt for modular systems that can grow with the company's business needs and have the capacity for cloud-based solutions to allow flexibility for remote access.
- v. All software will be aligned with the regulatory requirements, and ICT Department will ensure the software supports compliance with Kenya's Data Protection Act, Water Act 2016, and procurement regulations – particularly PPADA 2015. At minimum, the software should include audit trails, secure data storage, and customizable reporting formats.
- vi. In selecting the vendors for the required software, the company shall prioritize vendors with proven experience in Kenyan or East African context and who have available local technical support and training services.
- vii. The ICT department will advise MARWASCO management on the costs for acquisition, licensing, customization, training, and future upgrades of the essential software based on the Total Cost of Ownership (TCO) analysis, while considering software acquisition risks and potential mitigation measures as outlined in Table 2.

Table 2: Possible ICT Software Risks and potential mitigation measures

Risk	Description	Mitigation
Over-customization	Excessive tailoring can delay deployment and complicate upgrades.	Stick to core needs and modular add-ons.
Vendor Lock-In	Proprietary systems may limit flexibility and increase long-term costs.	Choose open standards and exportable data formats.
Poor Change Management	Resistance from staff or committees due to unclear benefits or lack of training.	Use participatory rollout and visual communication tools.

Risk	Description	Mitigation
Data Security Gaps	Non-compliance with ICT laws or weak encryption can expose sensitive data.	Conduct legal reviews and insist on secure hosting.
Underestimating Training Needs	Assuming users will adapt without structured onboarding.	Budget for iterative, localized training sessions.
Ignoring Offline Functionality	Systems that rely solely on internet connectivity may fail in remote areas.	Ensure offline data capture and sync capabilities.

5.4. Options for software acquisition by MARWASCO

MARWASCO will consider owning essential operational and technical software through several strategic pathways. The ICT Department will advise the management on the cost, control, and compliance implications of each pathway. The pathways anticipated are:

1. *Outright Purchase (Perpetual License)*, where the company pays a one-time fee to own the software indefinitely, especially for stable, long-term systems like billing, HR, or asset management to gain full control, reduce recurring costs and enhance offline usability.
2. *Subscription-Based Licensing (SaaS)*: Some software will be acquired through this method, where the company pays monthly or annually to access cloud-hosted software, particularly for GIS dashboards, leak detection, mobile data collection, and Computer Aided Design (CAD) software. The company may take advantage of lower upfront costs, automatic updates, and remote access.
3. *Custom Development (In-House or Outsourced)*: MARWASCO may also consider custom built software tailored to the company's operational needs, where there is need to integrate indigenous knowledge, visual toolkits, or unique workflows. This option will present the company with the option for full customization, local language support, and community-friendly interfaces.
4. *Open-Source Adoption*: The company may also acquire software for its needs by using and modifying free software under open licenses. This would be considered in case where licensed software is not affordable budget-wise, the company has requisite technical expertise to customize the software and there is need for flexibility and adaptation to local needs.
5. *Donor-Funded Acquisition*: MARWASCO will consider procuring some of the software through funded projects or partnerships if the software use is in line with the

project objectives or would complement the achievement of the grant's objectives. For example, AUTOCAD in infrastructure projects with extensive design elements. Where software is acquired through donor funding, training and support costs will be integrated into the purchase costs.

6. Public Sector Shared Services: In some cases, MARWASCO may consider use of platforms provided by national or county governments, particularly for compliance, reporting, and integration with national systems. In this case, the company will consider alignment with policy and reduce procurement burden.

5.5. Acceptable ICT Equipment and Software use practices

- a. The company devices will only be installed with licensed and approved software. Staff shall avoid pirated or unauthorized tools to minimize risk of data breach and reputational damage to MARWASCO.
- b. ICT resources must be used for MARWASCO's operational, technical, and administrative purposes only to support business continuity for the company services, including billing, reporting, GIS mapping, HR documentation, computer aided design, and stakeholder communication.
- c. Sensitive company data such as finance, customer database and proprietary information will be stored in encrypted formats with passwords protection to comply with Kenya's Data Protection Act.
- d. Each user will ensure that personal use of company devices is minimized and that use does not interfere with official work.
- e. All staff will use official email for work-related correspondence and access only relevant websites for company operations or research, and company issued mobile devices will be configured for field data collection, leak reporting, and community engagement apps.
- f. The use of social media during working hours will be limited to sharing verified updates on water and sanitation service delivery or public notices via official company social media handles / accounts with prior management approval.
- g. Loss of company asset due to negligence will be recovered through staff salary deduction on agreed terms between the Management and Staff.
- h. The ICT department will regularly update software and antivirus tools in MARWASCO devices and systems to prevent vulnerabilities. It is the staff's duty to report to ICT any need for updates arising outside the scheduled maintenance and upgrade schedules.

5.6. Non - acceptable practices Use of ICT Equipment and Software

To maximize the ICT resources for company's business, certain activities are prohibited during working hours including accessing inappropriate websites, downloading unauthorized software, streaming videos during working hours, and

sharing confidential company information. The following categories are considered non-acceptable practices as per this ICT Policy:

- i. Personal Use: Using company devices for personal entertainment, social media, or non-work-related browsing.
- ii. Data Misuse: Sharing customer data, financial records, or internal reports without authorization.
- iii. Unauthorized Access: Bypassing security protocols or accessing restricted systems without clearance.
- iv. Software Tampering: Installing unapproved apps, altering system configurations, or disabling security features.
- v. Cybersecurity Risks: Clicking suspicious links, downloading from unverified sources, or ignoring phishing alerts.
- vi. Social Media Misconduct: Posting unofficial statements, complaints, or internal matters on public platforms.
- vii. Negligence: Leaving devices unattended, failing to log out, or ignoring backup protocols.

The ICT Department will develop Standard Operating Procedures (SOPs) to operationalize this section of the policy, including acceptable and non-acceptable practices, reporting misuse of ICT equipment or software and actions to be taken to mitigate unacceptable practices.

5. Data Management and Security

MARWASCO as a public utility handling sensitive customer and operational data desires to move towards a culture of digital responsibility, aligning with Kenya's broader digital governance goals aimed at enhancing public trust as the organization expands digital services like mobile billing and online customer portals. The organization will undertake certain measures in line with Data Protection Act, to safeguard critical customer and staff data including:

5.1. Legal obligation to protect personal data.

In line with Data protection Act, 2019, MARWASCO will ensure that all personal data — such as customer names, ID numbers, billing records, mobile payment details, and supplier information is Collected lawfully and fairly; used only for specific, legitimate purposes; stored securely and access-controlled and is deleted or anonymized when no longer needed.

5.2. Mandatory data governance structures

MARWASCO will appoint a Data Protection Officer or designate internal “data champions” to oversee compliance and maintain clear records of data processing activities, ensuring staff are trained on privacy protocols and any breaches are addressed

through disciplinary procedures, as per Human Resources Policy and Procedures Manual.

5.3. Customers and transparency

As provided under Data Protection and Freedom of Information Act, customers will reserve their rights to access, correct, or request deletion of their personal data, facilitated by MARWASCO's personnel authorized to do so. MARWASCO will also provide clear privacy notices explaining how data is used and respond to data-related complaints and requests in a timely manner.

5.4. Breach notification and accountability

If MARWASCO experiences data breaches (e.g., unauthorized access to billing systems), the management will take immediate action to limit further breaches including:

- Notifying the Office of the Data Protection Commissioner
- Informing affected individuals / institutions promptly of nature, scale and implications of the data breaches, including actions taken by the company to address the situation.
- Conduct a comprehensive systems audit to establish the causes leading to the breach and make necessary recommendation to prevent similar breach in future.

5.5. Cybersecurity and system design

To mitigate against cybersecurity threats, systems used for billing, customer management, and mobile payments will include encryption, access controls, and audit trails.

MARWASCO will restrict and monitor staff access to sensitive systems to ensure system integrity and full compliance with the law.

5.6. Data minimization and retention

MARWASCO will only collect necessary data from its staff, customers and other clients, define clear retention schedules for customer and supplier records, and ensure old data is securely deleted or anonymized.

- i. Employees must use strong passwords and update them every 90 days.
- ii. Sensitive data, such as customer records and operational plans, must be stored in encrypted formats and accessed by authorized personnel for official use only.
- iii. Regular backups will be conducted to prevent data loss and ensure business continuity.

6. Cybersecurity and Data Protection

6.1 Overview

MARWASCO recognizes cybersecurity as a critical component of its ICT ecosystem, essential for safeguarding operational systems, customer data, and institutional integrity. This section outlines the company's commitment to secure digital practices in accordance with the Kenya's Data Protection Act (2019), Computer Misuse and Cybercrimes Act (2018), and the Critical Information Infrastructure Regulations (2024).

6.2 Governance and Accountability

The company shall establish a cybersecurity governance framework led by a designated ICT Security Officer. This framework will define roles, responsibilities, and escalation protocols for managing digital risks. Oversight will be provided by the ICT Sub Committee, which will ensure alignment with national legislation and sectoral standards.

6.3 Data Protection and Privacy

All personal, operational, and financial data shall be protected through encryption, secure storage, and access controls. MARWASCO shall ensure compliance with the Kenya Data Protection Act, including lawful processing, consent management, and breach notification procedures. Unauthorized access or information disclosure shall be subject to disciplinary process and legal action.

6.4 System and Network Security

The company will deploy firewalls, antivirus software, and intrusion detection systems across all ICT infrastructure. Regular vulnerability assessments and penetration testing shall be conducted. All software and firmware must be updated promptly to address known threats. Antivirus procurement shall follow PPADA guidelines and include centralized license management.

6.5 Incident Response and Recovery

MARWASCO will maintain an incident response plan detailing procedures for detection, containment, investigation, and recovery. All cybersecurity incidents must be logged and reported within 12 hours. Lessons learned shall inform future mitigation strategies and policy updates.

6.6 User Awareness and Training

All staff and contractors shall undergo regular cybersecurity training covering password hygiene, phishing awareness, and responsible data handling. MARWASCO shall promote a culture of digital responsibility and ensure users are equipped to recognize and respond to threats.

6.7 Third-Party and Vendor Compliance

All third-party service providers, including hosting, cloud, and software vendors—must demonstrate compliance with MARWASCO's cybersecurity standards. Contracts shall include clauses on data protection, breach notification, and audit rights. Vendors must cooperate with MARWASCO in the event of a security incident affecting shared systems.

6.8 Monitoring, Audit, and Continuous Improvement

The company shall implement continuous monitoring of ICT systems and conduct periodic audits to assess cybersecurity posture. Findings shall inform updates to policies, procedures, and infrastructure. MARWASCO shall remain responsive to emerging threats and evolving regulatory requirements.

7. Hardware and Software Management

MARWASCO will provide each member of staff with ICT company equipment for their work, configured to MARWASCO's standards. The equipment will be tagged for ease of tracking and details recorded in the company's asset register. The ICT department will be responsible for maintaining up to date ICT asset register.

Procurement of ICT equipment or devices will comply with National ICT Standards, which can be accessed at (<https://cms.icta.go.ke/>), tailored to MARWASCO's user needs by ICT department and in line with the Company's Procurement Policy.

Only personnel authorized by ICT Manager may install or modify software on MARWASCO devices.

Employees must report any hardware issues immediately to the ICT department and follow guidelines provided to resolve the issue.

Company ICT assets will not be repaired by third party vendors who are not vetted and approved by ICT Department.

On exceptional cases where personal devices are to be used for work, these devices must comply with MARWASCO's minimum security standards, including data storage access and dissemination.

8. Incident Reporting

Any ICT-related incidents, such as data breaches or system failures, must be reported to the ICT Department within 24 hours.

A detailed incident report will be prepared by the personnel affected by the incident for review and resolution by ICT department.

ICT Department will develop and roll out standard operating procedures for ICT related incident management.

9. Training and Awareness

In coordination with Human resources and user departments, the ICT department will conduct staff training needs assessments on information, communication and technology and roll out in-house training plan to equip staff with essential ICT use and management skills.

Induction for the newly recruited staff will include orientation to ICT policy by the ICT department.

All employees will receive annual training on ICT best practices, cybersecurity, and the use of ICT tools specific to water, sewerage, and sanitation management.

Company technical staff who require specific ICT tools and software for their daily work, will consult with ICT department for detailed specification, procurement, and installation in company devices.

The department may also arrange specific training for staff provided by the Equipment and Software sellers / dealers or institutions MARWASCO may have strategic partnerships with.

10. Implementation and Compliance with the ICT policy

The ICT department is responsible for the implementation of this policy, reviewing and updating when need arises and creating awareness among all staff and stakeholders engaged by the company.

All employees must adhere to this policy and relevant ICT laws, such as Kenya's Data Protection Act.

Failure to comply with the policy will lead to disciplinary action as per MARWASCO's Human Resources and Administration policy.

11. Monitoring and Review

- i. ICT usage will be monitored to ensure compliance and identify areas for improvement.
- ii. This policy will be reviewed and updated annually to align the policy with technological advancements, evolving regulatory requirements and MARWASCO's operational needs.
- iii. ICT Department will lead the process of review with the participation of the user departments and recommended changes approved by the Management and board of directors.

Annexes

Annex 1: MARWASCO ACCESS TO INFORMATION REQUEST FORM

Ref No: _____

1. Applicant Information

Full Name: _____

ID/Passport No: _____

Postal Address: _____

Physical Address: _____

Telephone: _____

Email: _____

2. Information Requested

Description of the nature of information sought:

Reason (s) or Purpose of the request:

Request Approved by MD: ☐ Yes ☐ No

If not Approved, reasons for declining request:

3. Preferred Method of Access

☐ Physical inspection

☐ Copies (digital or print)

☐ Email delivery

☐ Other (specify): _____

4. Declaration

I hereby declare that the information provided is accurate and the request is made in accordance with the Access to Information Act, 2016.

Name of Authorized Personnel: _____

Signature: _____

Date: _____

Official Company Stamp

Annex 2: Access to Information Compliance Checklist for MARWASCO

This checklist helps ensure MARWASCO meets its legal obligations under the Act:

Requirement	Status	Action Needed
Appointing an Information Access Officer	☐	Assign and train a staff member
Develop and publish an Access to Information Policy	☐	Draft and approve policy
Provide public access to request forms	☐	Upload to website and display at offices
Maintain a record of information requests	☐	Create and update regularly
Respond to requests within 21 days (or 48 hours if urgent)	☐	Set internal deadlines and reminders
Train staff on the Access to Information Act	☐	Conduct workshops or briefings
Proactively disclose key public interest information	☐	Publish reports, budgets, service updates
Establish appeal and complaint procedures	☐	Link with Commission on Administrative Justice
Protect confidential and exempt information	☐	Define exemptions and train staff
Monitor and review compliance annually	☐	Schedule internal audits and reviews

Annex 3: Decision Matrix for Software ownership Models

Ownership Model	Cost Profile	Customization	Control & Compliance	Community Usability	Scalability	Maintenance Responsibility
Perpetual License	High upfront	Moderate	High (local hosting, full control)	Moderate (requires training)	Limited	Internal IT or vendor
SaaS Subscription	Low upfront, recurring	Low–Moderate	Moderate (vendor-hosted, data sharing risk)	High (mobile-friendly, real-time)	High	Vendor-managed
Custom Development	High (initial + updates)	Very High	Very High (fully owned IP)	Very High (can include Swahili, icons)	High	Internal or contracted
Open Source	Low	High (if skilled team available)	Moderate (depends on hosting)	Moderate–High	High	Internal or community-supported
Donor-Funded	Zero direct cost	Low–Moderate	Low–Moderate (depends on donor terms)	High (often includes training)	Limited (project-bound)	Donor or short-term vendor
Shared Government Platform	Free or subsidized	Low	High (aligned with national standards)	Moderate	Moderate	Government agency

Annex 4: Asset Register Template

Organization Name: _____ County/Ward: _____

Date of Register Update: _____ Prepared By: _____

Asset Register – with Sample details (*Delete sample data and replace*)

#	Asset Code	Description	Asset Type	Location (GPS + Ward)	Acquisition Date	Condition	Assigned Officer	Warranty Expiry	Maintenance Schedule	Disposal Date	Remarks
1	WT-MBT-001	10,000L Water Tank	Water Infrastructure	GPS: -0.123, 37.456 / Ngurunit	2022-06-15	Good	John Mwenda	2025-06-15	Annual	—	Tagged & verified
2	ICT-MRS-015	HP Laptop (Core i5)	ICT Equipment	NDMA Office, Marsabit	2023-01-10	Fair	Mary Nkirote	2026-01-10	Quarterly	—	Antivirus active
3	BP-TUR-003	Borehole Pump – Lokichar	Water Infrastructure	GPS: 3.123, 35.789 / Lokichar Ward	2021-11-20	Needs Repair	—	2024-11-20	Biannual	—	Awaiting parts

Notes for Compliance

- Tag Format: Use QR or RFID with color - coded labels (Blue for water, Green for ICT, etc.).
- Data Protection: Avoid personal ID numbers; use staff names only with consent.
- Audit Trail: Keep digital logs of edits and physical verification reports.
- GIS Integration: Link GPS coordinates asset maps for visual tracking.



www.marwasco.co.ke



MARWASCOMARSABIT



info@marwasco.co.ke



254 726 689 803



@MarwascoM_bt



Marwasco offices, next to the office of the Governor, Marsabit

