



Maji Safi Kila Wakati

**KERICHO WATER & SANITATION
COMPANY LTD.
(KEWASCO)**

ICT POLICY

Version 1.5



*Accepted as true copy
of original
Kebii chepkoy side
msd
Chapman*

APPROVAL

This ICT Policy document in its initial form has received the following review and approvals from KEWASCO management:

Prepared By:

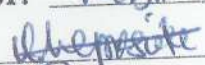
ICT Manager: RASTO CHEPKWONY

Signature: 

Date: 28/07/2021

Authorized by:

Managing Director: Kibii C. Seke

Signature: 

Date: 28/07/2021

Approved by:

Board of Directors

1. Chairperson:

Name: _____

Signature: _____

Date: _____

2. Board Member Representative:

Name: _____

Signature: _____

Date: _____

TABLE OF CONTENTS

KERICHO WATER & SANITATION COMPANY LTD.	i
(KEWASCO)	i
ICT POLICY	i
Version 1.5	i
2021 REVISION HISTORY	i
APPROVAL	iii
TABLE OF CONTENTS	iv
1.0 Introduction	1
1.1 Objectives	2
1.2 Scope	2
2.0 PASSWORD POLICY	3
2.1 Purpose	3
2.2 Scope	3
2.3 Policy	3
General	3
2.4 Password Construction Guidelines	4
2.5 Password Protection Guidelines	5
2.6 Enforcement	6
3.0 INTERNET USAGE POLICY	6
3.1 Introduction	6
3.2 Employee's Account	6
3.3 Appropriate Use	7
3.4 Inappropriate Use	8
3.5 Security	8
3.6 Failure to Comply	8
3.7 Monitoring and Filtering	8
3.8 Disclaimer	9
3.9 Bandwidth Utilization	10
4.1 Introduction	10
4.2 Scope	10
4.3 Account Activation/Termination	11
4.4 General Expectations of End Users	11
4.5 Appropriate Use	11
4.6 Inappropriate Use	13
4.7 Monitoring and Confidentiality	13
4.8 Reporting Misuse	13

4.9	Disclaimer	14
5.0	E-MAIL COMMUNICATION POLICY.....	15
5.1	Introduction.....	15
5.2	Subject Line.....	15
5.3	Length.....	15
5.4	Content.....	16
5.5	Attachments	16
5.6	Format.....	16
5.7	Style.....	17
5.8	Responding	17
5.9	Email etiquette.....	18
5.10	Email Signature.....	18
6.0	PRINTERS USAGE	19
6.1	Purpose	19
6.2	Scope.....	19
6.3	Supported Printers..	19
	Printer Model	20
6.4	General Policy	22
7.0	DOWNTIME POLICY.....	22
7.1	Purpose	22
7.2	Planned Downtime	23
7.3	Emergency Downtime.....	23
7.4	Notification of Downtime	24
7.5	Requests for Availability	25
8.0	SERVER BACKUP POLICY.....	25
8.1	Introduction.....	25
8.2	What is backed up.....	26
8.3	Backup Schedule.....	27
8.4	Managing Restores	30
9.0	INFORMATION TECHNOLOGY STANDARDS POLICY.....	30
9.1	Introduction.....	31
10.1	Purpose	31
10.2	Scope.....	31
10.3	General Policy	32
10.4	Rules for Virus Prevention.....	33
10.5	ICT Department Responsibilities	34
10.6	Department and Individual Responsibilities	35
10.6	Anti-virus software.....	35
	HARDWARE INFRASTRUCTURE STANDARDIZATION	38
10.7	Enforcement.....	39
11.0	Access Control Policy	39
11.1	Purpose.....	39
11.2	Scope	39
11.3	Policy	39

Role Based Access Control (RBAC) is a policy to be adopted since it grants access based on a user's role and implements key security principles, such as "least privilege" and "separation of privilege." Thus, someone attempting to access information can only access data that's deemed necessary for their role.	39
11.4 Access control Guidelines.....	39
11.5 Enforcement.....	40

1.0 Introduction

ICT (Information and Communication Technologies): ICT means technologies, including computers, telecommunication and audio-visual systems, that enable the collection, processing, transportation and delivery of information and communications services to users.

A Vision Statement: To have an organization which fully makes use of ICT in supporting the delivery of its services and creates the necessary framework (policies, legislations & regulations) that allows and utilize the full potential of ICT to be harnessed fully for the benefit of KEWASCO.

ICT Mission: Our mission is to supply technology and information services needed to fulfill the requirements in supporting KEWASCO corporate strategic plan now and in the future.

These services include but are not limited to:

- Providing, maintaining, and supporting hardware and software.
- Maintaining and providing access to mission critical data within a secure environment.
- Providing documentation, education and training for the KEWASCO staff.

ICT Policy: A policy is a deliberate plan of action to guide decisions and achieve rational outcome(s). Policy differs from rules or law. While law can compel or prohibit behaviors (e.g. a law requiring the payment of taxes on income) policy merely guides actions toward those that are most likely to achieve a desired outcome.

ICT System: An ICT system definition includes, but is not limited to, hardware, software and communications equipment that KEWASCO uses to communicate, process and store information. The organization and structures involved in relating all these systems, the information they store and the people involved in the administration and maintenance.

User: A user means any person who is recognized by KEWASCO as having a valid reason to access KEWASCO ICT systems whether that access is from within KEWASCO or outside KEWASCO

Alternate Site: Alternate Site means a site held in readiness for use in the event of a major disruption that maintains an organization's business continuity.

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations, KEWASCO is not an exception. While the board and the management of KEWASCO recognize this fact, organizations all over the world, including KEWASCO, are faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance. This ICT Policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by KEWASCO employees and KEWASCO business partners and customers plus other stakeholders.

1.1 Objectives

All KEWASCO's ICT facilities and information resources remain the property of KEWASCO and not of particular individuals, teams or departments. It is in view of this fact that the objectives of the policies are to:

- Enhance information security of KEWASCO systems.
- Enhance efficient use of information systems by KEWASCO employees and the affiliates.
- Enhance availability of ICT systems
- Enhance a spirit of awareness, co-operation, trust and consideration for others.
- Enhance compliance with the laws of Kenya.

1.2 Scope

The ICT policy document relates to all Information Technology facilities and services provided by KEWASCO including, but not limited to, email system, databases, ERP (Enterprise Resource Planning), operating systems (windows), internet, telephone systems, wireless communication, printers and copiers, just to mention a few. All KEWASCO employees, volunteers as well as business partners are expected to adhere to it. The document shall be effective from the date of approval.

2.0 PASSWORD POLICY

2.1 Purpose

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees of KEWASCO are required to take appropriate steps to ensure that they create strong, secure password and keep them safeguarded at all times.

The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

2.2 Scope

This policy applies to all employees of KEWASCO who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any KEWASCO facility, has access to the KEWASCO network, or stores any non-public KEWASCO information.

2.3 Policy

General

1. Passwords must be changed every 3 weeks.
2. Old passwords cannot be re-used for a period of 2 months.
3. Users will be notified 1 week in advance of password expiration date. At this time, users will be prompted to select a new password.
4. All passwords must conform to the guidelines outlined below.

2.4 Password Construction Guidelines

Passwords are used to access any number of company systems, including the network, Systems such as billing software, e-mail, and the Web. Poor, weak password are easily cracked, and put the entire system at risk. Therefore,

strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords should not be based on well-known or easily accessible personal information.
2. Passwords must contain at least 6 characters.
3. All passwords must start with a letter.
4. Passwords must contain at least 1 uppercase letters (e.g. N) and 2 lowercase letters (e.g. t).
5. Passwords must contain at least 2 numerical characters (e.g. 5).
6. Passwords must contain at least 1 special characters (e.g. \$).
7. A new password must contain at least 6 characters that are different than those found in the old password which it is replacing.
8. Passwords must not be based on a users' personal information or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.
9. Passwords must not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.
10. Passwords must not be based on the company's name or geographic location.

2.5 Password Protection Guidelines

1. Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members, under any circumstances.

2. If someone demands your password, refer them to this policy or have them contact the ICT Department.
3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's secured Virtual Private Network, FTP or SSL-protected Web site.
4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.
5. Do not use the "Remember Password" feature of applications e.g. when accessing Internet
6. Passwords used to gain access to company systems should not be used as passwords to access non-company accounts or information.
7. If possible, don't use the same password to access multiple company systems.
8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the ICT Department and the password changed immediately.
9. The ICT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

2.6 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.0 INTERNET USAGE POLICY

3.1 Introduction

The goals of this policy are to outline appropriate and inappropriate use of KEWASCO's Internet resources, including the World Wide Web, electronic mail, the intranet, and FTP (file transfer protocol). Your account provides you with access to networks around the world through these services. Use of these services is subject to the following conditions.

3.2 Employee's Account

Internet access at KEWASCO is controlled through individual accounts and passwords. Department managers are responsible for defining appropriate Internet access levels for the persons in their department and conveying that information to the network administrator.

Each user of the KEWASCO system is required to read this Internet policy and sign an Internet use agreement prior to receiving an Internet access account and password.

3.3 Appropriate Use

Individuals at KEWASCO are encouraged to use the Internet to further the goals and objectives of KEWASCO. The types of activities that are encouraged include:

1. Communicating with fellow employees, business partners of KEWASCO, and clients within the context of an individual's assigned responsibilities;
2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities;
3. Participating in educational or professional development activities.
4. Downloading software upgrades and patches.
5. Review of possible vendor web sites for product information.
6. Reference regulatory or technical information.
7. Research work to solve a particular technical problem

3.4 Inappropriate Use

Individual Internet use will not interfere with others' use and enjoyment of the Internet. Users will not violate the network policies of any network accessed through their account. Internet use at KEWASCO will comply with all Kenyan, regional and international laws, all KEWASCO policy, and all KEWASCO contracts. This includes, but is not limited to, the following:

1. The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
2. The Internet may not be used in any way that violates KEWASCO's policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of KEWASCO, misrepresents KEWASCO, or violates any KEWASCO policy is prohibited.
3. Individuals should limit their personal use of the Internet. KEWASCO allows limited personal use for communication with family and friends, independent learning, and public service. KEWASCO prohibits use for mass unsolicited mailings, access for non-employees to KEWASCO resources or network facilities, competitive commercial activity unless pre-approved by KEWASCO, and the dissemination of chain letters.
4. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to KEWASCO or another individual without authorized permission.
5. In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments.
6. Don't open email unless you have a reasonably good expectation of what it contains and the source of the mail, e.g. Do open report.doc from an Internet colleague you know, Don't open explore.zip sent from an address you've never heard of, however tempting. Alert IT Support if you are sent

anything like this unsolicited. This is one of the most effective means of protecting KEWASCO against email virus attacks.

3.5 Security

For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. Users are required to obtain a new password if they have reason to believe that any unauthorized person has learned their password. Users are required to take all necessary precautions to prevent unauthorized access to Internet services.

3.6 Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at KEWASCO. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of the Internet may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
2. Disciplinary action according to applicable KEWASCO policies;
3. Legal action according to applicable laws and contractual agreements;

3.7 Monitoring and Filtering

KEWASCO may monitor any Internet activity occurring on KEWASCO equipment or accounts. KEWASCO currently does not employ filtering software to limit access to sites on the Internet. If KEWASCO discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

3.8 Disclaimer

KEWASCO assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. KEWASCO is not responsible for the accuracy of information found on the Internet and only facilitates the accessing

and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

We encourage you to use your Internet access responsibly. Should you have any questions regarding this Internet Acceptable Use Policy, feel free to contact ICT department

3.9 Bandwidth Utilization

Users are therefore encouraged to use the available bandwidth to the interest of the company. The use of the following bandwidth intensive application **YOUTUBE, FACEBOOK, SPORTPESA, TORRENTS** and any other form of online streaming is prohibited during office hours as stated in the table below.

Office Hour	Period
8 am to 1 pm	Morning Session
2 pm to 5 pm	Afternoon session

4.0 E-MAIL USE POLICY

4.1 Introduction

E-mail is a critical mechanism for business communications at KEWASCO. However, use of KEWASCO's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of KEWASCO.

The objectives of this policy are to outline appropriate and inappropriate use of KEWASCO's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

4.2 Scope

This policy applies to all e-mail systems and services owned by KEWASCO, all e-mail account users/holders at KEWASCO (both temporary and permanent), and all company e-mail records.

4.3 Account Activation/Termination

E-mail access at KEWASCO is controlled through individual accounts and passwords. Each user of KEWASCO's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

All employees of KEWASCO are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Contractors.
- Board of Directors
- Suppliers

Applications for these temporary accounts must be submitted in writing to ICT Manager. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement.

E-mail access will be terminated when the employee or third party terminates their association with KEWASCO, unless other arrangements are made. KEWASCO is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

4.4 General Expectations of End Users

Important official communications are often delivered via e-mail. As a result, employees of KEWASCO with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business- and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove himself or herself from the list, and is responsible for doing so in the event that their current e-mail addresses changes.

E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.

4.5 Appropriate Use

Individuals at KEWASCO are encouraged to use e-mail to further the goals and objectives of KEWASCO. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of KEWASCO, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

4.6 Inappropriate Use

KEWASCO's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others' use and enjoyment of KEWASCO's e-mail

system and services. E-mail usage at KEWASCO will comply with all applicable laws, all KEWASCO policies, and all KEWASCO contracts.

The following activities are deemed inappropriate uses of KEWASCO systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of e-mail in any way that violates KEWASCO's policies, rules, or administrative orders
- Viewing, copying, altering, or deletion of e-mail accounts or files belonging to KEWASCO or another individual without authorized permission.
- Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 5 MB or less.
- Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.
- Excessive personal use of KEWASCO e-mails resources. KEWASCO allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. KEWASCO prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-KEWASCO commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

4.7 Monitoring and Confidentiality

The e-mail systems and services used at KEWASCO are owned by the company, and are therefore its property. This gives KEWASCO the right to monitor any and all e-mail traffic passing through its e-mail system. While the company does not actively read end-user e-mail, e-mail messages may be inadvertently read by ICT staff during the normal course of managing the e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with KEWASCO's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If KEWASCO discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of KEWASCO become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply", "Reply to All", "Forward" commands during e-mail correspondence.

4.8 Reporting Misuse

Any allegations of misuse should be promptly reported to ICT manager. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

4.9 Disclaimer

KEWASCO assumes no liability for direct and/or indirect damages arising from the user's use of KEWASCO's e-mail system and services. Users are solely responsible for the content they disseminate. KEWASCO is not responsible for any third-party claim, demand, or damage arising out of use the KEWASCO's e-mail systems or services.

5.0 E-MAIL COMMUNICATION POLICY

5.1 Introduction

The following are guidelines for drafting professional e-mail communications. These guidelines should be followed to ensure a professional online image and to conserve network bandwidth and server storage space.

5.2 Subject Line

A poor subject line could cause your e-mail to be dumped in the trash.

- Write "information-rich" subject lines. Say exactly what the e-mail is about.
- Avoid exclamation marks and words like "Urgent." They quickly lose their effect.

5.3 Length

The briefer the e-mail, the more likely the chance it will be read in full.

- Stick to one screen (i.e. 25 lines, or 250 words). If you need more space, then e-mail may not be the right medium – consider phone or fax instead.
- If you absolutely must send a longer e-mail, add the word "Long" to the subject line so that your reader is prepared or include the bulk of your content in an attachment.

5.4 Content

Your ultimate goal is to ensure your content is read and understood.

- If the recipient doesn't know you, include your name, occupation, and employer.
- Focus on one subject per e-mail. Send several messages if you have multiple topics to cover.
- Get to your point by the second sentence.

- Use absolute dates and times (e.g. "Monday, December 5 at 2:00" instead of "this afternoon" or "tomorrow", etc). If communicating between time zones, set a reference.
- If you're including a URL, type it out in full (i.e. <http://...>). A URL is also more valuable and bandwidth-friendly than sending a copy of the Web page.
- Sign your e-mail and include a signature file with your contact information. With so many viruses, signing assures your recipient that the message is from you.

5.5 Attachments

Attachments, while a valuable tool could cause problems at the recipient end due to viruses, download time, or poor translation. Use them judiciously.

- Only send attachments when absolutely necessary and with the permission of the recipient (especially if the attachment is over 50K).
- If you have multiple attachments, send each in a separate message with an appropriate subject line to make them easier for the recipient to track and retrieve.

5.6 Format

The format or layout of your e-mail serves to maximize readability.

- Use numbers and bullets to recap or list agenda and action items.
- Write a series of brief paragraphs, and always insert a line between them.
- Avoid all-caps – it comes across as shouting. If you need emphasis, put asterisks on either end of the word or phrase. Conversely, avoid typing in all lower-case.

5.7 Style

Style is the hardest element to master. Too rigid, and you could come off as humorless and intimidating. Too casual and you may be dismissed as someone not to be taken seriously.

- Know your audience. This will dictate the level of formality required. A "business casual" tone will suit most occasions. Think "khakis and a golf shirt."
- Avoid acronyms like TIA (thanks in advance), JAM (Just A Minute) or BTW (by the way). A lot of people will have no ideas what these mean.
- Avoid making jokes – they often misfire.

5.8 Responding

E-mail communication is a two-way street. Responding to e-mail in a professional manner is just as important as being a good e-mail writer.

- Don't reply unless it is required in some way. Don't spam the sender's inbox.
- Respond to e-mail messages promptly. If you need more time, send a brief acknowledgement telling the sender when you'll respond in full.
- Always refer back to the content in the sender's original e-mail. Quote them.
- Consider "interweaving" your response within the sender's original text, especially if they want feedback on multiple issues. This makes it clear what item you are addressing in your response.

5.9 Email etiquette

- Do address someone by name at the beginning of the message, especially if you are also copying another group of people i.e. be courteous
- Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.
- Don't open email unless you have a reasonably good expectation of what it contains and the source of the mail, e.g. Do open report.doc from an Internet colleague you know, don't open explore.zip sent from an address

you've never heard of, however tempting. Alert IT Support if you are sent anything like this unsolicited. This is one of the most effective means of protecting KEWASCO against email virus attacks.

- Understand how forwarding an email works. If you forward mail, it appears (to the reader) to come from the originator (like passing on a sealed envelope). If you forward mail *and edit it* in the process, it appears to come from you - with the originator's details usually embedded in the message. This is to show that the original mail is no longer intact (like passing on an opened envelope).

5.10 Email Signature

- When sending emails to suppliers customers etc using the company's' email the user must ensure the use of the following standard formatting and the use of circulated signature at all times

Kind Regards

Your name | Designation

KERICHO WATER & SANITATION CO. LTD

PO Box 1379 - 20200 Kericho, Kenya | ☎+254 734778931/ 0721777416 | ☎Fax: +254 05230583

☎Direct Line: +254 | ☎Mobile: Private Mobile Number | company_mail@kewasco.co.ke

www.kewasco.co.ke



Guiding Principle;

"One person working alone is limited in their endeavours; many people working together have no limit to their Achievements"

The information contained in this e-mail is confidential, may be legally privileged and is intended solely for the addressee.

If the reader of this communication is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this communication in error and that any use, review, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete this e-mail and any copy thereof.

6.0 PRINTERS USAGE

6.1 Purpose

Printers represent one of the highest equipment expenditures at KEWASCO. The goal of this policy is to facilitate the appropriate and responsible business use of KEWASCO's printer assets, as well as control KEWASCO's printer cost of ownership by preventing the waste of paper, toner, ink, and so on.

6.2 Scope

This Printer Policy applies to all employees of KEWASCO, as well as any contract employees in the service of KEWASCO who may be using KEWASCO networks and equipment.

6.3 Supported Printers

KEWASCO supports the printers named in the table below. An effort has been made to standardize on specific printer models in order to optimize contractual agreements and minimize support costs. The table indicates the model, resolution, location, and capabilities (e.g. color printing, double-sided printing, large print jobs, and special paper types) of all KEWASCO printers.

Printer Name	Printer Model	Resolution (dpi)	Location	Capabilities
HP Laserjet	2015d	600-1200	Billing Office	27ppm, Duplex
HP Laserjet	2015d	600-1200	Customer Care	27ppm, Duplex
Hp Laserjet	2055d	1200	MD's Sec	Over 30 ppm
Hp Laserjet	2055d		Procurement, Salaries	
Hp Laserjet	2055d		Accounts	
HP Deskjet	8055		MD's and P& E offices	3-in-1
Deskjet	J740		CM's and HRM's Offices	
Epson			Cashier	Printing receipts
Thermal	TEP -2220		Cashier	Printing receipts

* The list of printers is subject to change

6.4 General Policy

1. Printers are to be used for documents that are relevant to the day-to-day conduct of business at KEWASCO. KEWASCO printers should not be used to print personal documents.
2. Installation of personal printers is generally not condoned at KEWASCO due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is at issue, personal printers may be allowed.
3. Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.
4. If you print something, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e. recycle).
5. If you come across an unclaimed print job, please stack it neatly in printer output box. All unclaimed output jobs will be discarded after 2 days.
6. Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing six or more PowerPoint slides per page versus only one per page).
7. Make efforts to limit toner use by selecting light toner and lower dpi (dots per inch) default print settings.
8. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Please report any planned print jobs in excess of 200 pages to the ICT department so that the most appropriate printer can be selected and other users can be notified.
9. If printing a job in excess of 50 pages, please be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).

10. Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
11. Avoid printing a document just to see what it looks like. This is wasteful.
12. Avoid re-using paper in laser printers, when installed, as this can lead to paper jams and other problems with the machine.
13. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with ICT or the table above to find out which machines can handle these specialty print jobs.
14. Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.
15. Printer paper and toner cartridges are available at main store or ICT department and can be obtained using duly filled Request Voucher.
16. If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not "trained" in how to fix the problem, please do not try. Instead, report the problem to ICT or ask a trained co-worker for help.
17. Report any malfunction of any printing device to ICT department as soon as possible.

7.0 DOWNTIME POLICY

7.1 Purpose

KEWASCO is committed to ensuring reliable information technology services. In order to meet this objective, KEWASCO systems may need to be taken offline to maintain or improve system performance, safeguard data, or to respond to emergency situations.

The goal of this policy is to explain those circumstances during which downtime may occur, anticipated durations of downtime events, and procedures for notifying affected users.

7.2 Planned Downtime

From time to time, it will be necessary to make systems unavailable for the purpose of performing upgrades, maintenance, or housekeeping tasks. The goal of these tasks is to ensure maximum system performance and prevent future system failures. The following activities fall within the definition of Planned Downtime:

- Application of patches to operating systems and other applications in order to fix vulnerabilities and bugs, add functionality, or improve performance.
- Monitoring and checking of system logs.
- Security monitoring and auditing.
- Disk defragmentation, disk cleanup, and other general disk maintenance operations.
- Required upgrades to system physical memory or storage capacity.
- Installation or upgrade of applications or services.
- System performance tuning.
- Regular backup of system data for the purpose of disaster recovery.

In the event that any of these activities will require downtime to perform, every effort will be made to perform the procedure during off-hours in order to minimize the impact on those who use the affected systems or services. The following time periods will be used to carry out Planned Downtime activities:

- Weekdays – After 5.00 PM
- Saturday – After 1.00 PM
- Sunday – Whole day

On occasion, it may be necessary to have Planned Downtime during regular business hours, namely if outside personnel are required to perform more elaborate procedures. If this is the case, then this Planned Downtime will be communicated to identified users of affected resources using the Notification of Downtime mechanism described below.

7.3 Emergency Downtime

Unexpected circumstances may arise where systems or services will be interrupted without prior notice. Every effort will be made to avoid such circumstances. However, incidences may arise involving a compromise of system security, the potential for damage to equipment or data, or emergency repairs. If the affected system(s) cannot be brought back online with 15 minutes affected users will be contacted via the Notification of Downtime mechanism described below.

7.4 Notification of Downtime

Users will be notified of downtime according to the following procedure:

- The ICT Manager is responsible for notifying all identified users of Planned Downtime, as well as any unplanned interruptions to system availability as they occur.
- The ICT Manager will first notify all affected users via memos and e-mail or an intranet bulletin board. All users are responsible for checking the mentioned methods for downtime and system status notifications. In the event that the intranet bulletin board is unavailable due to Emergency

Downtime, the system administrator will contact department heads by SMS or telephone to inform them of the situation.

- If general maintenance procedures will cause Planned Downtime during regular business hours, and the procedure will last less than 30 minutes, then the ICT Manager must notify system users 1 hour prior to the Planned Downtime.
- If Planned Downtime beyond general maintenance is scheduled that will last longer than 5 hours, then the ICT Manager must give 2 business days notice for every day of anticipated system unavailability. This step must be taken regardless of whether the downtime is scheduled to take place during off hours or regular business hours.
- In the event of Emergency Downtime, the ICT Manager will use his/her discretion in notifying end users of the situation. In emergency circumstances where time is of the essence, it may not be possible for the ICT Manager to engage in normal downtime notification activities.

All downtime announcements will provide the following information:

- Systems and services that are affected, as well as suggested alternatives to them (if any).
- Start and end times of the Planned Downtime period, or estimated time to recovery in the event of Emergency Downtime.
- The reasons why the downtime is taking place.
- Any ongoing problems that are anticipated as a result of the downtime event.

7.5 Requests for Availability

If you foresee critical need of a system during a period of Planned Downtime, then contact ICT department in advance to make an appeal. The utmost effort will be made to reschedule the downtime or make alternative arrangements for required resources.

8.0 SERVER BACKUP POLICY

8.1 Introduction

Data is one of KEWASCO's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

8.2 What is backed up

This policy refers to the backing up of data that resides on KEWASCO's servers. Servers and the files and/or data types on these servers that are covered by this policy include:

- Billing System Database M@jics database.
- Sage Pastel Database
- Payroll System database Isoft
- Cloud SYNC Database
- Any other company's Information System

This policy does not refer to backing up of data that resides on individual PC or notebook hard drives. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to the appropriate server listed above in order that their data is backed up regularly in accordance with this policy.

In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications, prior to the backup procedure window.

It is the responsibility of server administrators to ensure that all new servers be added to this policy, and that this policy be applied to each new server's maintenance routine. Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.

8.3 Backup Schedule

Backups are conducted both manually/automatically].

The softwares listed above must be backed up according to the following procedure. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:

1. All backup tapes are to be labeled using the following labeling conventions:
 - Name-dd.mm.yyyy (e.g Payroll-01.12.2010)
2. All backup tapes stored on site are to be stored outside the organization [Name withheld for security reasons]
3. All backups will take place at the end of transaction every day. This timeframe has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the IT Department so that exceptions or alternative arrangements can be made.
4. Incremental backups (only files changed since the last backup) will be performed daily, Monday through Saturday. These tapes will be stored onsite during the following backup cycle.
5. A full backup will be performed every Saturday. This tape will be stored on site during the following backup cycle.

6. A full backup will be performed at the end of each month. This tape will be immediately removed to a predetermined offsite location for permanent storage. These tapes will never be reused.

7. All server backups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labeled three-ring binder in an agreed-upon, centralized location. The log must include:

- Server name,
- Date and time of backup,
- Name of administrator performing the backup,
- Files backed up and/or skipped,
- Software used to perform the backup,
- Backup medium used and its label/name, and
- Whether the backup was successful or not.

8. If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed by 9:00 A.M the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, end users in the organization must be notified.

9. If a tape is discovered to be damaged or corrupt, then the tape must be destroyed to prevent further use and replaced with a new one.

8.4 Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential to regularly test one's ability to restore data from its storage media.

1. All daily tapes must be tested at least once every 2 months to ensure that the data they contain can be completely restored.
2. All weekly tapes must be tested at least once every 3 months to ensure that the data they contain can be completely restored.
3. All monthly tapes must be tested at least once every 2 years to ensure that the data they contain can be completely restored.

Data will be restored from a backup if:

- There is an intrusion or attack.
- Files have been corrupted, deleted, or modified.
- Information must be accessed that is located on an archived backup.

In the event a data restore is desired or required, the following policy will be adhered to:

1. The individual responsible for overseeing backup and restore procedures is System administrator or ICT Manager. If a user has a restore request, they can contact ICT Department by calling , sending an e-mail or filling out and submitting a request form
2. In the event of unplanned downtime, attack, or disaster, consult KEWASCO's Disaster Recovery Plan for full restoration procedures.
3. In the event of a local data loss due to human error, the end user affected must contact the IT Department and request a data restore. The end user must provide the following information:
 - Name.
 - Contact information.
 - Name of file(s) and/or folder(s) affected.
 - Last known location of files(s) and/or folder(s) affected.
 - Extent and nature of data loss.

- Events leading to data loss, including last modified date and time (if known).
 - Urgency of restore.
4. Depending on the extent of data loss, a daily tape, weekly tape, or combination of both will need to be used. The timing in the cycle will dictate whether or not these tapes are onsite or offsite. Tapes must be retrieved by the server administrator or pre-determined replacement. If tapes are offsite and the restore is not urgent, then the end user affected may be required to wait up to [insert time frame] for a time- and cost-effective opportunity for the tape(s) to be retrieved.
5. If the data loss was due to user error or a lack of adherence to procedure, then the end user responsible may be required to participate in a tutorial on effective data backup practices.

BACKUP REPORT DETAILS

DATE	1/12/2014	2/12/2014	3/12/2014	4/12/2014
TIME				
PF NO.				
NAME				
M@JICS				
EVOLUTIONCOMMON				
SAGE PASTEL				
CLOUDSYNC				
PAYROLL				
LOCATION1				
LOCATION 2				
SIGNATURE				

9.0 INFORMATION TECHNOLOGY STANDARDS POLICY

9.1 Introduction

The Information Technology Standards Policy lists all technologies supported by the organization and serves as a guideline for all technology purchasing and use decisions, including hardware, software, peripherals, and network components. The primary goals of developing and implementing such a policy are:

- To ease purchasing decisions by pre-evaluating and pre-approving technology solutions.
- To reduce training and support costs and create economies of scale by narrowing the number of technologies and products used.
- To ensure integration and interoperability between technologies.
- To set parameters for future technology innovation and development.

The following standard technologies were selected based on prevalence in the organization or – in the case where two or more competing technologies previously existed – on an assessment of relative quality and performance as dictated by business needs.

Please refer to this document when making a purchasing decision or when selecting technologies as part of a development project. Sections of this document may be extracted and used as part of project charters or other agreements where technology parameters should and must be set, such as in the case of contracted work.

10.0 ANTI-VIRUS POLICY

10.1 Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, flash disks/sticks, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to KEWASCO in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of KEWASCO is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by KEWASCO employees to help achieve effective virus detection and prevention.

10.2 Scope

This policy applies to all computers that are connected to the KEWASCO network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the KEWASCO network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

10.3 General Policy

1. Currently, KEWASCO has 47 (14 CDs 3-User for PCs and Laptops and 5-User for the Server) Licensed Kaspersky Antivirus. The most current available version of the anti-virus software package will be taken as the default standard.
2. All computers attached to the KEWASCO network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

3. Any activities with the intention to create and/or distribute malicious programs onto the KEWASCO network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
4. If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the ICT department immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.
6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

10.4 Rules for Virus Prevention

1. Always run the standard anti-virus software provided by KEWASCO.
2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. Files with certain filename extensions are blocked by the e-mail system.
6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7. Avoid direct disk sharing with read/write access. Always scan a removable drives such as flash disks for viruses before using it.
8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

10.5 ICT Department Responsibilities

The following activities are the responsibility of the KEWASCO ICT department:

1. The IT department is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted at FTP server. Check one of these locations regularly for updated information.
2. The IT department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use every week.
3. The IT department will apply any updates to the services it provides that are required to defend against threats from viruses.
4. The IT department will install anti-virus software on all KEWASCO owned and installed desktop workstations, laptops, and servers.
5. The IT department will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. The IT department may provide anti-virus software in these cases depending on the availability of free licensed anti-virus that has not been utilized.

6. The IT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
7. The IT department will perform regular anti-virus sweeps of certain system(s) files.
8. The IT department will attempt to notify users of KEWASCO systems of any credible virus threats via e-mail, memos or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

10.6 Department and Individual Responsibilities

The following activities are the responsibility of KEWASCO departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
2. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
3. All employees are responsible for taking reasonable measures to protect against virus infection.
4. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the KEWASCO network without the express consent of the IT department.

10.6 Anti-virus software

With respect to anti-virus software:

- (i) The head of ICT shall ensure availability and continuous update of anti-virus protection on all computers, laptops and servers;
- (ii) No person shall be allowed to connect private PCs, laptops, modems or any ICT peripheral to KEWASCO network or hardware without permission from ICT Department;
- (iii) All removable media in use within KEWASCO must be scanned for viruses.

HARDWARE INFRASTRUCTURE STANDARDIZATION

Desktop Computers

- (i) KEWASCO shall seek to:
 - (a) Standardize hardware equipment to minimize multi brands;
 - (b) Allocate computers to user departments appropriately;
 - (c) Provide uninterrupted power supply and protection to all ICT installations in order to protect the systems from power fluctuations and surges; and
 - (d) Review hardware specifications to be in line with current technological trends.
- (ii) Users are accountable for all ICT equipment allocated to them.

Laptops

With respect to Laptops:

- (i) Laptops will be procured for functional areas and assigned to officers whose nature of work merits their use;
- (ii) Hardware specifications will be reviewed to be in line with current technological trends;
- (iii) Users are accountable for all laptops issued to them; and

(iv) There will be no additional software installation without prior authority from the Head of ICT.

Servers

The following best practices will be adhered to with respect to server deployments within KEWASCO:

- (i) Maximization of the storage system;
- (ii) Ensuring online and offsite backups and real-time replication for critical applications;
- (iii) Disaster prevention arrangements.
- (vi) The acquisition of servers should be standardized to avoid multi brands;
- (vii) All servers other than for backing up and disaster recovery shall be located in a central server room;
- viii) The head of ICT will be responsible for the administration of all the servers in the KEWASCO;
- (ix) Provide uninterrupted power supply and protection for all servers; and
- (x) Review hardware specifications to be in line with current technological trends.

Procurement

The procurement of hardware, software, peripherals and network products shall be guided by procurement laws and regulations and:

- (i) Must conform to minimum specifications and standards established by the head of ICT;
- (ii) Must be informed by annual procurement plans.
- (iii) Take into account software requirements and anticipate future requirements;
- (iv) The MD will approve direct procurement of ICT emergency equipment.
- (v) Be from manufacturers, authorized dealers and/or certified service centers.
- (vi) Must have warranty.

Inventory

(i) KEWASCO shall establish and maintain an inventory of all ICT equipment in the functional areas.

(ii) In the event of movement of officers occasioned by deployment or exit, the head of the affected functional area shall reallocate any ICT equipment under

their custody and communicate the same to the head of ICT, for purposes of updating the inventory.

(iii) Movement of ICT hardware (PCs, printers and scanners) from one office to another shall be done in consultation with KEWASCO asset management office and the head of ICT to enable the updating of asset register as result of change of location

Installation

On installation of information technology products:

(i) An Installation Certificate must be issued and signed by the head of ICT who shall be involved in the entire installation process;

(ii) The head of the functional area shall be responsible for all installations; and

(iii) All installations must be in accordance with the supplier standards and KEWASCO requirements; Operation

(i) All operations must have User and Technical manuals from the supplier;

(ii) The operating environment must conform to the minimum manufacturers' specifications or international standards; and

(iii) Emergency procedures must be clearly displayed in the server room and data center.

Maintenance of ICT equipment

Maintenance of ICT equipment is critical for effectiveness and efficiency of KEWASCO operations. The following policy will therefore apply:

(i) ICT hardware purchased must have Service Level

Maintenance Agreements on expiry of the warranty;

(ii) Only certified manufacturer authorized agents will be allowed to provide maintenance,

(iii) Internal maintenance shall be provided by personnel trained and certified.

(iv) Maintenance contracts for ICT equipment shall be managed by the head of ICT.

Decommissioning of ICT equipment

With respect to decommissioning ICT equipment:

- (i) All ICT equipment shall have a predetermined life span;
- (ii) There must be written justification by the head of ICT for decommissioning of any ICT equipment;
- (iii) Equipment that are no longer effective or in use will be decommissioned within 6 months after the review;
- (iv) ICT equipment will be decommissioned after an installation certificate has been issued for replaced systems;
- (v) A decommissioning Certificate will be issued on successful conclusion of the exercise.

Disposal

Information technology resources disposal must:

- (i) Be in accordance with the existing public disposal rules and regulations;
- (ii) Avoid or minimize degradation to the environment;
- (iii) Seek to re-use some of or all the computer components;
- (iv) Seek authority to donate any retired computer equipment;
- Remove data and systems on all hardware to be disposed of;
- (vi) Comply with manufacturer, supplier or service provider terms and conditions of disposal; and
- (vii) Be indicated on the Disposal Certificate.

10.7 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including denial of computer services or even termination of employment.

11.0 Access Control Policy

11.1 Purpose

ACCESS CONTROL IS A TOOL we can use to help secure systems. Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances. For instance, policies may pertain to resource usage within or across organizational units or may be based on need-to-know, competence, authority, obligation, or conflict-of-interest factors

The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

11.2 Scope

This policy applies to all employees of KEWASCO who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any KEWASCO facility, has access to the KEWASCO network, or stores any non-public KEWASCO information.

11.3 Policy

Role Based Access Control (RBAC) is a policy to be adopted since it grants access based on a user's role and implements key security principles, such as "least privilege" and "separation of privilege." Thus, someone attempting to access information can only access data that's deemed necessary for their role.

11.4 Access control Guidelines

1. Inventory your systems

Figure out what resources you have for which you need to control access, if you don't already have them listed. Examples would include an email system, customer database, contact management system, major folders on a file server, etc.

2. Analyze your workforce and create roles

You need to group your workforce members into roles with common access needs. Avoid the temptation to have too many roles defined. Keep them as simple and stratified as possible.

For example, you might have a basic user role, which might be a customer service rep, that would have read/write access to the customer database, and a customer database administrator, that would have full control of the customer database.

3. Assign people to roles

Now that you have a list of roles and their access rights, figure out which role(s) each employee belongs in, and set their access accordingly.

4. Never make one-off changes

Resist any temptation to make a one-off change for an employee with unusual needs. If you begin doing this, your RBAC system will quickly begin to unravel. Change the roles as required or add new ones when really necessary.

5. Audit

Periodically review your roles, the employees assigned to them, and the access permitted for each. If you discover, for example, that a role has unnecessary access to a particular system, change the role and adjust the access level for all employees in that role.

11.5 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



*Confirmed as true copy
of original
Kibii Chelwayi Siale
MSD*