Information Communication Technology (ICT) Policy

TABLE OF CONTENTS

1.0. Preamble

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations. Rak Unity is not an exception. While the Board and the Management of Rak Unity recognize this fact, organizations all over the world, including Rak Unity, 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 both Rak Unity employees and Rak Unity business partners.

2.0. Objectives

All Rak Unity's ICT facilities and information resources remain the property of Rak Unity Petroleum Plc and not of particular individuals, teams or departments (Note 1). It is in view of this fact that the objectives of this document are thus to:

I. Enhance compliance with the laws of Federal republic of Nigeria.

II. Enhance information security of Rak Unity systems.

III. Enhance best practice according to international Standard Organization.

IV. Enhance efficient use of information systems by Rak Unity employees and the affiliates.

V. Enhance availability of ICT systems.

VI. Enhance a spirit of awareness, co-operation, trust and consideration for others.

3.0. Scope

The ICT policy document relates to all Information Communication Technology facilities and services provided by Rak Unity including, but not limited to, email system, databases, accounting application operating systems (Windows and UNIX), internet, telephone systems, wireless communication, printers and copiers. All Rak Unity employees, volunteers as well as business partners are expected to adhere to it. The document shall be effective from the date of approval.

4.0. Precautionary and Disciplinary Measures

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include the offender being denied access to computing facilities.

4.1 Copyright: Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

4.2 Security:

4.2.1 Don't attempt to gain unauthorized access to information or facilities. It is an offence to obtain unauthorized access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact your IT Support person or provider through the helpdesk system.

4.2.2 Don't disclose personal system passwords or other security details to other staff, volunteers or external agents and don't use anyone else's login; this compromises the security of Rak Unity. If someone else gets to know your password, ensure you change it or get IT Support to help you (Note 2).

4.2.3 If you leave your PC unattended without logging off or locking the session, you are responsible for any misuse of it while you're away.

4.2.4 ALWAYS check flash disks for viruses, even if you think they are clean (Contact ICT support for help). Computer viruses are capable of destroying Rak Unity's information resources. It is better to be safe than sorry.

4.3 Information about people: If you're recording or obtaining information about individuals makes sure you are not breaking Data Protection legislation (your Manager can guide you on this).

4.4 You are a representative of Rak Unity when you are on the Internet using email:

4.4.1 Make sure your actions are in the interest (and spirit) of Rak Unity and do not leave Rak Unity open to legal action (e.g. libel).

4.4.2 Avoid trading insults with other people using the Internet with whom you disagree.

4.4.3 Obscenities/ Hate, violence, etc.: Don't write it, publish it, look for it, bookmark it, access it or download it.

4.5 **Electronic Espionage**: Any information available within ICT facilities must not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are: In the case of a specific allegation of misconduct, when the Management Team can authorize accessing of such information during the course of investigation. This may necessitate disabling the victim from accessing ICT facilities pending investigation. When ICT Support section cannot avoid accessing such information whilst fixing a problem, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary.

5.0. Email Policy

5.1 When to use email:

5.1.1 Use it in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. Think and check messages before sending (just as you would a letter or paper memo).

5.1.2 Use the phone (including voicemail if no reply) for urgent messages (email is a good backup in such instances).

5.1.3 Use Rak Unity's intranet (not email) to communicate all relatively static information (e.g. policy, procedures, briefing documents, reference material and other standing information).Record information on the intranet in a well-structured manner, (consulting with the Web Systems Administrator as appropriate). Use email merely as a pointer to draw attention to new and changed information on the intranet.
5.1.4 Use Rak Unity's intranet shall never at any time be used to send personal messages

5.2 Use of Distribution Lists:

5.2.1 Only send Email to those it is meant for; don't broadcast (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer and network performance and wastes disc space.

5.2.2 Use the standard aliases (Note 3) for work related communication only.

5.2.3 If you wish to broadcast other non-work related information or requests (e.g. information or opinions on political matters outside the scope of Rak Unity's campaigning, social matters, personal requests for information etc.) it is better to use a Webmail account (Note 4) or a personal email account at home; don't use the standard (work) aliases.

5.2.4 Keep Rak Unity's internal email aliases internal. If you are sending an email both to a Rak Unity alias and outside of Rak Unity, use the alias as a blind carbon copy (i.e. the bcc address option) so that the external recipient does not see the internal alias.

5.2.5 Don't broadcast emails with attachments to large groups of people - either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

5.3 General points on email use:

5.3.1 When publishing or transmitting information externally be aware that you are representing Rak Unity and could be seen as speaking on Rak Unity's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

5.3.2 Check your inbox/in-tray at regular intervals during the working day. Keep your in-tray fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

5.3.3 Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.

5.3.4 Use prefixes in the subject box whenever appropriate (Note 5).

5.3.5 Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicize their displeasure at the actions / decisions of a colleague).

5.3.6 Don't forward emails warning about viruses (they are invariably hoaxes and systems administrators will probably already be aware of genuine viruses - if in doubt, contact them for advice). Exception: Only Systems administrators can forward warnings about viruses.

5.4 Email etiquette:

5.4.1Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are also copying another group of people.

5.4.2 Make your subject headers clear and relevant to your reader(s) e.g. don't use subject headers like "stuff" Don't send a subject header of, say "accounts" to the accountant.

5.4.3 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.

5.4.4 Using asterisks at each end of a word (e.g. *now*) is common practice for highlighting text.

5.4.5 Capitals (e.g. NOW) can also be used to emphasize words, but should be used sparingly as it commonly perceived as 'shouting'.

5.4.6 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 Rak Unity against email virus attacks.

5.4.7 Keep email signatures short. Your name, title, phone/fax and web site address may constitute a typical signature.

5.4.8 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).

5.5 Delivery & Receipt of Mails

The nature of email is very controversial, as while a certain mail may be SPAM to one person it may not be SPAM to another. There are lots of SPAM filtering software out in the market, but none is perfect. There are always cases of some mails being passed out by the software as being clean while it is not clean (*false positives*) or being rejected as SPAM while it is not SPAM *(false negatives)*. This controversy is further complicated by the fact that there are many parties involved in a mail. For a mail to be successfully delivered it entails that:

1. The sender uses the correct address.

2. The internet of the sender is up.

3. The internet of the recipient is up.

4. That the sender’s organization server has no technical problems.

5. That the recipient’s organization mail server has no technical problems.

6. That the sender’s PC is online.

7. That the recipient’s PC is online.

8. That the anti-spam software recognizes it appropriately.

It is due to this complexity that, urgent mails should be given at least 15 minutes for delivery and followed up through telephone. Users receiving NDR (Non-Delivery Reports) for mail failures shall forward the same to ICT Support or ICT Systems Administrators for trouble shooting. Staffs are however required to ascertain, before launching a complaint that the address of the recipient is correct and free from typos. Complaints about mail receipt failure should always be accompanied by the sender address and the recipient address. This will enable the administrators to narrow down to the particular case and give a report and advice to the affected user the soonest possible (within 30 minutes or as per the SLA).

6.0. Internet Policy

Only users authorized through their line managers are allowed to browse during work time. Other users can browse after working hours and during weekends. Users shall not assume any privacy while browsing the internet. Browsing is always monitored and some sites are restricted by use of internet monitoring software. Any user who is blocked from accessing a site which facilitates his work can, through his/her line manager, get in touch with systems administrators to open up the site as long as the site is safe to access and does not compromise Rak Unity network. Hate, violence, etc. are always blocked.

7.0 Network Security and Access Policy

Firewalls and Intrusion Detection systems shall be used across the entire Rak Unity network to monitor and prevent hackers, viruses and worms including all other forms of attach. The in-charge of network shall ensure that this policy is adhered to. Failure to do this may necessitate disciplinary action depending on circumstances and top management approval. All computers hooked into the network shall mandatorily have up-to-date antivirus software to prevent viruses and all other forms of malicious code. Additionally the computers must have all unnecessary services disabled to prevent intrusion. It shall be the responsibility of ICT support to ensure that this policy is adhered to failure to which disciplinary action shall be executed as per management approval. All staff is also expected to seek authority from ICT support before hooking non company laptop to o the network.

8.0 Data Centre and DRC Access Policy

Only authorized ICT personnel are allowed to access the ICT data center and DRC. All other persons must be accompanied by authorized staff and must sign a visitor’s book. Responsibility: Senior Systems Administrator and his/her appointee. Consequence: Disciplinary action on the staff violating this policy.

9.0. Policy on Printers, Telephone lines, fax and Copiers.

Staffs are expected to use the above responsibly**.** Irresponsible/ excessive use of the above for personal purposes is discouraged, and may, depending on the line manager's determination and management's approval lead to disciplinary action which may include, but not limited to, denial of the service.

10.0. Policy on Passwords

10.1 Do not disclose to anyone (See Note 2 below)
10.2 Do NOT write it down.
10.3 Should be a combination of alphanumeric and special characters (!_?$^*#), i.e. complex, but easy to remember.
10.4 Passwords must be at least six (6) characters.
10.5 Users are required to change their passwords at least every three months. 10.6 Passwords shall lock for every three unsuccessful attempts.
10.7 The maximum number of sessions per user shall be three (3).
10.8 Password Management

I. This shall be the responsibility of Senior Systems Administrator (SSA) and/or his appointee(s).

II. A user whose password has expired, or account locked shall (upon request through IT support) be assigned an initial password by the systems administrator. The affected user must change the initial password immediately for security reasons; bearing in mind that users are solely responsible for actions committed using their own accounts.

11.0. Policy on ICT Related Training

11.1 Every section within ICT department shall identify training needs every beginning of financial year and forward to the ICT divisional committee.

11.2 The ICT divisional committee shall analyze the trainings relevant for every section to make sure that the training requirements are relevant to the various sections staff and within budget and forward the names and requirements to the manager in charge of ICT.

11.3 The manager in charge of ICT shall, upon his approval, forward the training requirements to Human Resource and Administration for implementation.

12.0. Policy on Online Subscriptions

12.1 Section heads shall have the mandate to do online subscriptions on behalf of their

sections, but in consultation with the manager in charge of ICT department. For security reasons, the section heads shall use their own money or cards to subscribe and only receive re-imbursements upon presentation of prove of payment.
12.2 Section heads are advised to be careful when making online payments/subscriptions as Rak Unity shall NOT be liable for any losses incurred through online/internet transactions.

13.0 Policy on ICT Disaster Recovery

ICT Disaster recovery shall be carried out as outlined in the ICT Services Disaster Recovery Plan which shall be provided by the Head, ICT

14.0 Policy on ICT Technical Assistance Request & Complaints.

All ICT technical assistance requests shall be channeled through the centralized helpdesk system. Requests and/or complaints made through other means e.g. telephone shall be given less priority than requests made through the helpdesk system. Responsibility: All staff.

15.0. Prohibition on use of personal devices
No employee of the company is allow to use any personal devices such as flash drive, hard disk, CD ROM, CD/DVD and any other storage devices on the company IT infrastructure.
In the event that use of personal device is absolutely necessary, approval and authorization will be obtained from Head, ICT with recommendation from Head, Business Unit.

16.0 Miscellaneous

16.1 Hardware and Software: All purchases should be approved by the ICT Manager, through the ICT budget.
16.2 Installing Software: Get permission from ICT Support or ICT Administrators before you install any software (including public domain software - see Note 6) on equipment owned and/or operated by Rak Unity.
16.3 Data transfer and storage on the network:
16.3.1 Keep master copies of important data on your profile e.g. My Documents folder. Otherwise it will not be backed up and is therefore at risk. This applies to managers. If you change your computer, you should inform ICT support to update the DLO agent which facilitates backup of your profile. Personal files should be kept to minimum.
16.3.2 Ask for advice from ICT Support and/or ICT Administrators if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill. (See Appendix I: Best Practices on transmitting attachments & pictures)
16.3.3 Be considerate about storing personal (non- Rak Unity) files on Rak Unity's network. (Note 7).
16.3.4 Don't copy files which are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disc space unnecessarily.

16.4 Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, playing computer games and browsing the Internet) is permitted so long as such use does not:

- Incur specific expenditure for Rak Unity
- Impact on your performance of your job (this is a matter between each member of staff and their line manager)
- Break the law
- Bring Rak Unity into disrepute.

16.5 Care of equipment:

- Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting ICT Support.
- Don't take food or drink into rooms which contain specialist equipment like servers (Note 8). Access to such rooms is limited to systems administrators and other authorized staff.

17.0. Revision

This policy shall be revised on a yearly basis. Changes necessitating revision shall include changes in technology, statutory regulations and any other reasons as may be determined from time to time by the manager in charge of ICT.

18.0 Approval

	Name	Job Title	Signature	Date
Prepared By	**Akinjobi Simeon**	**Head of Audit**		
Authorized By	**Engr. J. Ogungbemi**	**Managing Director**		
Approved By		**Board Director**		

NOTES

(1) In-house software: This is software written by staff or volunteers using Rak Unity's equipment. It is Rak Unity's property and must not be used for any external purpose. Software developers employed at Rak Unity are permitted to take a small "portfolio" of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to agreement with the ICT Manager.

(2) Personal passwords: Disclosure to other staff, volunteers or external agents: This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with the ICT Support. If the password is disclosed for a one-off task, the owner must ensure that his / her password is changed (by contacting ICT Support) as soon as the task is completed. Users shall be prompted to change their passwords from time to time to enhance system security.

(3) Email aliases are pre-defined 'shortcuts' for distributing internal email to specific groups of people. Systems administrators can tell you what these are and how to use them.

(4) Webmail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser, e.g. home or cybercafé. ICT Support can advise you on setting up such an account.

(5) Subject box prefixes: These are ''U:' for Urgent', 'FYI' for your information and 'AC:' requires action, ‘FYI:’ For Your

Information, ‘FYA:’ For Your Action. If the email is a very brief message confined solely to the subject line, it should in addition be prefixed with '**' to indicate "just read this line".

(6) Public domain software or Freeware: This is software that is available free of charge, usually by downloading from the internet.

(7) Personal Data: As a guideline, keep your personal data to minimal say 1GB. Ten emails require 0.15MB on average (depends a lot on whether they have attachments). A 10-page word processed document requires about 0.1MB. Screen saver images require much more disc space and vary greatly - some may be as large as 2MB.

(8) Computer Room/Data Center: This is the room in Rak Unity building which contains servers and communication equipment. The door should be closed at all times and entry restricted to authorized persons only.

ABBREVITAIONS

Rak Unity – Rak Unity Petroleum Plc.
DRC – Disaster Recovery Center/Site
ICT – Information Communication Technology
IT – Information Technology
FYI – For Your Information
NDR – Non Delivery Report
FYA - For Your Action
SLA – Service Level Agreement
ISO – International Organisation of Standards