The Information Technology & Telecommunications Policy

Kenya Power

THE INFORMATION TECHNOLOGY & TELECOMMUNICATIONS POLICY

Kenya Power

NOTICE

This policy document is the property of Kenya Power and describes the IT&T equipment and facilities management as applied to the operations of the company. Reproduction of this manual, in part or as a whole, is not permitted without the authorization of the General Manager, IT&T.

The information contained in this policy document may not be divulged or used for any other purpose other than that intended. The procedures described and related documentation shall not be regarded as legally binding upon the Company.

The right is reserved to amend the contents of this policy document and the procedures referred to therein to reflect any changes to circumstances, methods or products which may apply from time to time.

Contents

1. INTRODUCTION

1.1 Information Technology & Telecommunications Policies Document (ITP) Review Record

This is the third version of the Information Technology & Telecommunications Policy Document (ITP). The changes include reference number and the effective date and were necessitated by the need to update the policies for relevancy.

ITP REVIEW RECORD

DOCUMENT'S REVIEW RECORD		
DOCUMENT NAME	EDITION	EFFECTIVE DATE
Information Technology and Telecommunications Policy	Edition 1	
Information Technology and Telecommunications Policy	Edition 2	April 2007
Information Technology and Telecommunications Policy	Edition 3	March 2015

The Information Technology & Telecommunications Policy document provides the policies and procedures for handling ICT affairs in the company. It is prepared in conformity with legal requirements, industry regulations and ICT management best practices applicable to Kenya Power.

This manual is intended to be a working tool for managers and staff that they use to build a common understanding with their employees. It is the principal responsibility of each Departmental General Manager, Manager of Division and

Controlling Chief Engineer/ Analyst to ensure that each employee under their care acquaints themselves with the company's ICT policies and procedures and to correctly interpret this to the employees and ensure compliance.

These policies shall serve to ensure security of ICT resources, optimum usage and prevent any wastage of time, energy and resources.

These ICT policies and procedures also establish goals and form the basis of controls that govern all the operational units in the entire ICT department. The policies and procedures in this document are not the end in themselves but are a means to effective, efficient and transparent handling of ICT matters in the company.

The KPLC IT&T Policy team, which the team responsible for documenting, issuing and reviewing this Manual welcomes any comments and suggestions aimed at improving the IT&T Policy document.

1.2 Preamble

Numerous changes have taken place since the release of the last *Information Technology and Telecommunications Policy of April 2007*. This Policy is developed to capture recent changes that have taken place such as inclusion of MPESA payments, payment through banks, virtual networks, and so on. Security in use of IT&T facilities and equipment has become crucial and this Policy contributes in minimization and mitigation of any threat to the continuous provision of the essential IT&T services.

The Policy provides Kenya Power stakeholders and especially the IT&T facilities and equipment users with the guidelines for use of the facilities and how they are held to account for the use or misuse of the same. It is hoped that the document will go a long way in protecting the company business against malpractices and ensure smooth flow of information

and data that is needed to serve customers in the contemporary and future digital world. To this end, constant improvement of the document will be made to reflect any new change in the IT&T sector.

This Policy in its complete form replaces the previous *IT&T Policy document second Edition of April 2007*.

There are important attachments to this IT&T Policy documents. One of this is the *Norms and Procedures* document of October 2009 that gives detailed processes used to do various tasks. The other reference is the *ISO Procedures* that also depicts the same and is stored in the company's database *Q-pulse* for access by the relevant personnel. Another attachment is the *Disaster Recovery Plan* document of 2007 and the *IT&T Security Policy of 2015 document (draft)*.

1.3 Statement of Purpose

This Policy document serves as a guide to the users of IT&T facilities and equipment and prescribes the boundaries within which decisions can be made. The objectives of the Policy are to:

a) Ensure minimization of risk in the use of IT&T facilities and equipment and to indicate mitigating methods where risks exist.

b) Ensure implementation of security requirements in the use of IT&T facilities and equipment.

c) Provide users with standards to abide by.

d) Provide a framework for development, management and control of the various IT&T networks and systems.

e) Ensure compliance with the necessary statutes, regulations, and mandates in the running of every section of the IT&T Division.

f) Uphold the image and integrity of the company through use of the defined standards and guidelines.

1.4 Scope of the IT&T Policy

This Policy applies to all Kenya Power stakeholders that use the company's IT&T facilities. These include any person that may access, develop, implement, test, commission and use any IT&T based information owned, managed, supported or operated by, or on behalf of Kenya Power and Lighting Company. Hence all employees, contractors engaged by the company to carry out projects, develop, repair or maintain the IT&T resources, suppliers of IT&T resources and customers shall comply with the policies stipulated in this document.

2. DEFINITIONS AND ABBREVIATIONS

ACS – Access Control Server

ADR – Alternative Dispute Resolution

CCK – Communications Commission of Kenya

CET – Chief Engineer Telecoms

CM – Chief Manager

Contractor – Any person or firm that KPLC has engaged to provide a specific service or goods

CPU – Central Processing Unit

CRO – Customer Relations Officer

CSA – Chief Systems Analyst; for central office IT operations. In the regions, CSA functions shall be handled by/ through the Regional IT&T Engineer

DMZ – Demilitarized Zone

Hardware – The physical aspect of computers, telecommunications and other devices

HR – Human Resource

IT – Information Technology

ICT – Information and Communication Technology

IP – Internet Protocol

IRU – Indefeasible Right of Use

IT&T – Information Technology and Telecommunications

KPLC – Kenya Power and Lighting Company Limited

LAN – Local Area Network

MD & CEO – Managing Director and Chief Executive Officer

M-Pesa – Mobile money transfer service provided by Safaricom

NAT – Network Address Translation

NFP – Network Facility Provider

NMS – Network Management System

ODF – Optical Distribution Frame

OLTE – Optical Line Terminal Equipment

PIN – Personal Identification Number

PLC – Power Line Carrier Equipment

PSC – Power System Communication

RFQ – Request for Quotation

RTU – Remote Terminal Unit

SAS – Substation Automation Systems

SATIS – KPLC's Asset Management System

SCADA – Supervisory, Control, Access and Data Acquisition

SHE – Safety, Health and Environment

SLA – Service Level Agreement

Software – Includes Operating Systems, utilities and programs

Syslog – System Log

TBU – Telecoms Business Unit

TC – Tender Committee

Third party – Any person or firm that KPLC provides a service to

UHF – Ultra High Frequency

UPS – Uninterruptible Power Supply

User – Any person authorized to use IT&T facilities or systems

VLAN – Virtual Local Area Network

VPN – Virtual Private network

Non-Disclosure Agreement – An agreement entered into by two or more parties in which some or all of the parties agree that certain types of information that pass from one party to the other or that are created by one of the parties will remain confidential

3. I.T&T HARDWARE POLICY

3.1 New Hardware

a) Users shall be issued with an Assignment Note which they shall sign upon receipt of every IT&T hardware i.e. rugged laptop, tablets, workstations, laptop, personal computer, printer and scanner, IP Phone, Blackberry, Ipad, Portable Radios and Mobile Radios.

b) Users should be allocated new hardware in accordance with the following eligibility levels : –

i) Ipads and Blackberries will be issued as per the Telephone Policy on gadgets in the *HR Corporate Telephone Policy document of 2013*.

ii) Laptops, personal computers, printers and scanners will be issued to all levels of employees based on the following yearly user requirements : –

- Departmental/Section heads should forward their staff requirements to CSA/ Regional IT&T heads.
- IT support staff shall verify the need for user hardware replacement or disposal.
- All the recommendations for user hardware replacement or disposal shall be forwarded to CSA.

iii) Rugged laptops, tablets, workstations and other specialized user IT Hardware will be issued to employees upon request to I.T Manager through Divisional Managers.

iv) IP Phones, Portable/Mobile Radios will be issued to all levels of employees upon request to CET through the user's immediate supervisor.

3.2 Returning Hardware

Users shall be issued with a Receipt Note which shall be signed upon returning any issued IT&T Hardware.

3.3 Hardware Movement

a) Users shall be issued with a gate-pass during inter-depot movement of any IT&T hardware.

b) Any IT&T equipment leaving any KPLC facility either for repair or being carried away by a third party or contractor shall be issued with a gate-pass.

c) Returned hardware shall be verified to ascertain that it is in its intended condition before being accepted.

3.4 Lost Hardware

a) Users shall report any lost hardware to the Insurance Office. User should present their signed Assignment Note to the Insurance Office who will advise on any other requirements. At the same time, the user will report to the police and get a police abstract – a copy of which will be given to the company security officer with the regional office or in central office.

b) The CSA shall provide procurement information on the lost item i.e. Invoice Number, Purchase Order to the Insurance Office for purposes of reimbursement.

c) User may be surcharged for the lost item either fully or partially depending on the circumstances leading to the loss.

3.5 Inventory Control

a) All new hardware shall be keyed into the SATIS which is the Assets Management System.

b) A stock take shall be conducted every month of June in the financial year by Regional Heads of IT&T and in Central office by CSA or CET and the results verified in the SATIS.

3.6 Retirement of Obsolete I.T Hardware Policy

a) The process evaluation of IT hardware to determine whether it is more economical to repair, upgrade or replace IT hardware components shall be done every month of June in the financial year or upon approval by CSA for the purposes of disposing obsolete equipment.

b) IT hardware shall be considered obsolete if the estimated cost of repair exceeds one–half of the current estimated value or they are damaged beyond repair.

c) IT&T hardware and their accessories are considered uneconomical to maintain if the total cost of running them exceeds 60% of the cost of replacement and compatible replacements are not readily available.

d) Obsolete IT&T hardware will be disposed off as stipulated by the *Public Procurement and Disposal Act of 2005*.

3.7 Retirement of obsolete PSC and SCADA equipment

a) PSC and SCADA software, hardware and systems shall be declared obsolete according to the recommendations of the manufacturer. The PSC and SCADA maintenance teams, both in the regions and central office, shall periodically conduct maintenance to identify, retire and replace the hardware categorized as at "end-of-life."

b) A storage facility shall be identified in all regions for the collection and documentation of obsolete and failed PSC and SCADA equipment and a Tender Committee paper prepared at least once a year for the disposal of obsolete and failed equipment as per the *Public Procurement and Disposal Act of 2005.*

4. CONTRACTOR MANAGEMENT POLICY

a) An SLA describing the services to be offered, performance measurement, incident management, suppliers and KPLC duties, and the rules of engagement between the suppliers offering the IT&T services to be signed by the supplier and the CSA/CET.

b) A Scope of Work document describing tasks to be completed by a supplier in an IT&T Project, the location of work, period of performance, deliverable schedules, and acceptance criteria to be signed by the supplier and the CSA/CET before commencement of any IT&T project.

c) A Sign Off document describing accomplished tasks completed by a supplier in respect of the Scope of Work document to be signed by the supplier and the CSA/CET.

d) Department/Section Heads responsible for contractors should request for user creation on company systems for the authorized contractors to access company systems.

e) Authorized contractors' computers should have minimum technical hardware and software specifications approved by CSA/CET.

f) Different user accounts convention and user access matrix should be formulated for contractors.

g) Authorised contractors working on IT&T equipment shall sign a Non-Disclosure document.

5. BACKUP POLICY

5.1 Systems Backup

a) Backup copies of essential business data and software shall be taken regularly to ensure that all essential business data and software can be recovered following a computer disaster or media failure, and the backup copies shall be regularly checked to ensure that they can be relied upon in an emergency. A minimum level of backup information, together with accurate and complete records of the backup copies, shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the Data Centre.

b) At least three generations of backup data must be retained for important business data, software and applications. System Administrators shall establish and formally document an appropriate schedule for full and incremental backups.

c) Back-up data must be given a level of physical and environmental protection, consistent with standards applied at the main site. The controls applied to media at the main site must be extended to cover the Back-up site.

d) To safeguard against loss of data, the database must be operated in ARCHIVE-LOG mode and with a multiplexed Online Redo log. In order to ensure high-availability of the database, it should always operate in ARCHIVE-LOG mode to take advantage of Online Data file backups.

e) If data is lost due to external factors, such as fire or water damage to the hardware, or physical errors e.g. hardware failure, the database would have to be recovered up to the point in time when the database crashed. If a full recovery were possible, only the data of uncommitted transactions before the error would be lost.

f) If the data is lost due to logical errors, such as an unintentionally deleted table, the database must be recovered up to a point in time shortly before the error occurred.

g) The total recovery time, after loss of data, consists of the time necessary for:-

   i) Analysing the error;

   ii) Replacing the required hardware, and setting up the operating system and required file systems;

   iii) Restoring the database from data backups;

   iv) Performing a forward recovery from backed up redo log files;

   v) Performing an instance recovery automatically at system start-up.

h) Additional backups shall always be taken after structural change to the database and/or operating system's file system so as to ensure successful restores in the event that database or system crash (failure) occurs after the structural change and before scheduled backup.

i) Changes to the file structure of the database or operating system's file system affect the subsequent restore. These changes occur when a data file is added, a data-file is moved to a different location, or when a table space and its data-file are reorganised. In these cases the control file is changed and now different from the control file contained in the last backup. However, in case of a restore, the control file of the backup might be used and the file structure recorded in this control file is different from the actual file structure.

j) To facilitate recovery to a past point-in-time to correct an erroneous operational change to the database, ensure to run in ARCHIVE-LOG mode and perform control file backups whenever making structural changes. Having a backup control file that reflects the database structure

at the desired point-in-time facilitates recovery to a past point-in-time.

k) All systems (both applications and the database) will be backed up as per the backup schedule maintained by the systems production section.

l) Periodic restores will be done on the test environment to ensure correctness and integrity of the backup media devices/tapes.

5.2 SCADA System Backups

5.2.1 Responsibility

a) The CET shall formulate and implement systematic schedules for performing regular backups on key company systems. The responsible staff shall arrange to perform backups as scheduled at all times.

b) SCADA system backup shall be handled as outlined in Policy item 5.1(a)

5.2.2 Back-up Inventory File

a) IT&T shall maintain a Back-up Inventory file, which shall document all backups carried out on the critical systems. This shall provide mechanisms for quick monitoring and tracking of scheduled back-ups.

b) The following information shall be documented for all generated data backups :-

   i) Date and time the data backup was carried out (dd/mm/yyyy: hh:mm);

   ii) The name of the system or short description of the nature of the data;

   iii) Extent and type of data backup (files/ directories, incremental/full);

   iv) Backup hardware and software used (computer name, operating system (OS), version number);

v) Sequence number if any (where multiple removable backup media are used);

vi) Physical location of the server and the logical path on file-system to the back-up area, when fixed media (hard-disks) are used;

vii) Data restoration procedures shall be as set out in the Norms and Procedu*res document of 2009.*

The above information shall be filed in the back-up inventory file.

6. MAINTENANCE POLICY

System maintenance includes any activity which requires a system or systems to become unavailable to users for a period of time for the purpose of upgrading, reconfiguring, modifying, replacing or changing it, and servicing. Maintenance includes, but is not limited to software changes, hardware changes, network changes, patches, fixes or cabling.

6.1 General Maintenance Policy

a) IT&T teams will schedule any planned systems maintenance at a time which has the lowest impact on the company. They will be scheduled outside the normal company hours of operation.

b) Written notice of all scheduled maintenance of a significant nature shall be provided to clients/ customers, stating the nature of the change, system impact as well as documenting the starting time and duration of the maintenance.

c) Clients/customer representatives and other impacted stakeholders shall be notified when the required maintenance is completed and system operations have been restored.

d) Appropriate system maintenance logs and documentation shall be updated and reviewed after every maintenance.

e) Scheduled Maintenance shall be carried out by IT&T personnel as per Maintenance Program approved and circulated by the CSA/CET.

f) Breakdown Maintenance shall be carried out as per the norms and procedures outlined in the IT&T Norms and P*rocedures document of 2009*.

6.2 Preventive Maintenance Policy

a) Preventive Maintenance for user computers and printers shall be conducted twice yearly.

b) Preventive Maintenance for servers, routers, switches, air –conditioners and cooling systems, UPS and batteries and fire detection and suppression equipment shall be conducted every quarter of the year.

c) Preventive Maintenance for PSC and SCADA systems shall be conducted twice yearly.

d) Other Preventive Maintenances shall be carried out by contractors as per existing SLA/contracts.

6.3 Comprehensive Maintenance Policy

Comprehensive maintenance for IT&T equipment will be carried out as per agreed SLAs.

6.4 Maintenance Policy on User Hardware

a) Only IT&T support staff are authorised to install or modify software and to transfer and update data on company hardware. Any other persons shall require specific authorisation.

b) Installation manuals and media must be kept and readily available to the staff that are authorised to support or maintain systems.

c) Only authorised and licensed software will be installed on hardware.

6.5 Maintenance Policy on Software

a) IT Manager shall advise on system upgrades.

b) Systems software will be regularly maintained to ensure they meet the changing requirements of the various divisions and changes in technology.

c) New systems being installed must have been tested in the test environments and passed all quality checks. A test and quality check checklist will be maintained indicating the test results.

d) For internal developments, a change request/ transport request form must be filled and it must be duly signed for the change to be effected.

e) For systems maintained by contractors, a Service Level Agreement has to be maintained and any maintenance will be carried as per the Service Level Agreement.

6.6 Maintenance of PSC and SCADA Equipment

a) Any changes to substation layout or incorporation of new equipment shall be communicated to the CET for assignment to PSC personnel.

b) Only designated members of the staff of IT&T are authorized to install, operate and maintain active network equipment including PLC terminal equipment, OLTE, radios, communication media, RTUs and SASs. Requisite limitation of access issued by the control centre shall need to be obtained by authorized IT&T personnel.

c) In the case of contractors, installation and maintenance of active network equipment including PLC terminal equipment, OLTE, radios, communication media, SCADA servers, switches, routers, RTUs and SASs, requisite limitation of access issued by the control centre shall be obtained and supervision done by an authorized KPLC PSC representative. In cases where contractors have been authorized by the SHE department to carry out such installation works, no direct supervision at site will be required.

7. INCIDENT MANAGEMENT AND RESOLUTION POLICY

7.1 Incidences on I.T&T Hardware

a) Management of incidences will be guided by the procedures in the *IT&T Norms and Procedures docum*ent o*f 2009 and ISO 2008 procedure for IT&T hardware.*

b) All IT&T user incidences shall be logged in the IT&T service desk system. In cases where users experience difficulty, the incidences should be reported through the support desk extensions, or through the respective regional support help desk email addresses.

c) Head of support shall distribute the support desk incidences and ensure that each incidence is resolved within the set resolution time.

d) Users to be sufficiently informed of the IT&T service catalogue and escalation matrix for each service.

e) System incidences to be reported and resolved as indicated in the IT&T Norms and Procedures doc*ument of 2009.*

7.2 Incidences on Portable and Mobile VHF Radios

a) Radio equipment and communication failure shall be reported to the CET for allocation to IT&T resource personnel for trouble-shooting and resolution.

b) During trouble-shooting and resolution of a radio failure, the user shall be allocated another radio to use temporarily if available, to be returned when radio failure is resolved.

c) In the case of unresolvable radio failure, a new radio shall be assigned to the user and the old one recovered. ISO 2008 Procedure for allocation of IT&T hardware shall be followed accordingly.

d) No external radio shall be configured for use within the KPLC radio network.

8. USER ACCOUNT MANAGEMENT POLICY

a) Supervisors should formally make requests for user account creation for their staff to the relevant IT&T Section Head for approval.

b) All user accounts must be uniquely created. The first three characters of an account are prefixed 'kpl' followed by five-digit staff number, with exception of service accounts that have the 'kpl' prefix then followed by the service name. Contractors' accounts shall have the contractor's ID number.

c) User accounts that are unused or inactive for thirty days are automatically locked or disabled.

d) Users shall be granted privileges that are commensurate with their roles and responsibilities in the IT&T systems.

8.1 ADMINISTRATIVE ACCOUNT OR SPECIAL ACCESS ACCEPTABLE USE POLICY

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

The purpose of the Administrative Account or Special Access Acceptable Use Policy is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

Policy Guidelines

a) Kenya Power departments must submit to IT&T a list of administrative contacts for their systems that are connected to the company's network.

b) All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.

c) Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege.

d) Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate for work being performed (e.g. user account vs. administrator account).

e) Each account used for administrative/special access must meet the Kenya Power Password Policy.

f) The password for a shared administrator/special access account must change when an individual with the password leaves the department or Kenya Power or upon a change in the vendor personnel assigned to the Kenya Power contract.

g) In cases where a system has only one administrator, a password escrow procedure must ensure that someone other than the administrator can gain access to the administrator account in an emergency situation e.g. via use of securely kept password envelopes.

h) When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they must be:

- authorized;
- created with a specific expiration date;
- removed when work is complete.

i) All non-KPLC users (under item h) must sign a Kenya Power Non-Disclosure Agreement (NDA) before account access is enabled.

9. PASSWORD POLICY

a) Passwords shall be used on all Kenya Power automated information systems to uniquely identify individual users.

b) Be at least six characters in length.

c) Password complexity design shall be incorporated in all IT&T systems to include at least two of the following: upper case, lower case, special characters and numbers.

d) Passwords should not be shared amongst users. Generic, system defaulted or group passwords shall not be used. Password history should be set to the last 5 passwords in all IT&T systems.

e) To preclude password guessing, an intruder lock-out feature shall suspend accounts after three invalid attempts to log on; manual action by an administrator after user verification is required to reactivate the account.

f) Passwords shall expire after every 30 days.

g) Not be dictionary words.

h) Not be portions of associated account names (e.g. user ID, log-in name, personal information).

i) Not be character strings (e.g. abc or 123).

j) Not be simple keyboard patterns (e.g. QWERTY, asdf).

k) In addition, users are required to select a new password immediately after their initial log in.

l) Users are responsible for the security of their password(s) and are accountable for any misuse.

m) Incidents where a user suspects that his/her accounts has been compromised shall immediately be reported to the IT Security.

n) Any default passwords must be changed on all systems prior to connection to any network, even in pre-deployment testing.

o) Screen-saver password must be enabled after 5 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.

p) Vendor or service accounts will be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation at Kenya Power facilities.

10. INTERNET POLICY

a) Supervisors shall formally request for internet rights for their staff to the CSA for approval.

b) Use of internet resources for reasonable non-business purposes remains entirely subject to CM IT&T discretion and may be withdrawn on a temporary or permanent basis at any time.

c) Use of internet provided by KPLC (whether for personal or business purposes) may be monitored and recorded. Such monitoring will be for the purposes of KPLC maintaining its security and the proper operation of KPLC systems.

d) Internet resources shall not be used for purposes which are illegal, unethical or unacceptable.

e) Downloads of documents, executable files and zipped files will be subjected to malware scanning before download can commence.

f) Use of the internet for non-business high volume traffic over the network which might substantially hinder other users is prohibited e.g. streaming media (audio, radio or video) or heavy software downloads.

11. EMAIL POLICY

a) Supervisors shall formally request for company e-mail provision for their staff to the CSA for approval.

b) Company email shall not be used to send chain e-mails which may generate unnecessary high volume traffic in the KPLC Exchange Server environment.

c) User should not reply to unsolicited e-mails received at a KPLC Email address as this could allow the sender to verify addresses for purposes of sending a virus or hacking in KPLC system.

d) Automatic forwarding of company email to personal external email addresses is prohibited.

e) KPLC may monitor the use and content of any email generated, stored and/or handled on its systems for the purpose of detecting malware, spam and viruses.

f) KPLC may monitor the use and content of any email generated, stored and/or handled on its systems when required to do so by a government authority, legal or regulatory authority, KPLC security or KPLC audit departments.

g) Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of KPLC, or contain any material that is detrimental to any party outside the specific business interests of the company.

h) KPLC email systems are principally provided for business purposes.

12. ACCESS AND SECURITY POLICY

Access to all information systems must be logged and monitored to identify misuse of systems or information.

12.1 Network Access

a) All access to KPLC's network (via wired, wireless & VPN) shall be controlled by KPLC Domain Controller/Active Directory.

b) Temporary/Guest access shall be facilitated on request to CSA.

c) A guest account with appropriate permissions, with automatic date and time of expiry shall be activated for temporary use by the guest on approval by the CSA.

d) On resignation/termination of employment, employees will have their network access terminated during the clearing process.

12.2 Access to SCADA NMS

a) New System Controllers shall have their profiles created in the SCADA NMS on application from the relevant System Control Functional Head to the CET.

b) All System Controllers shall be required to change their passwords from the default password as soon as they are created within the SCADA system.

c) All System Controllers shall be required to perform "shift logins" at the beginning of their shifts so that the system can log their access into the network.

d) All System Controllers shall not run the system under super user rights as this is reserved only for authorised IT&T staff who are allowed to make system changes.

e) System Controllers shall not share their passwords with each other and shall be liable for any operations carried out in the power system under their profiles.

12.3 Data Access Monitoring

a) All networked systems providing network services or applications are monitored where relevant for:-

   i) CPU Utilization and active processes;

   ii) File store – utilization, anomalies, file types and file sizes;

   iii) Licensed software violations;

   iv) Network statistics e.g. peak and average bandwidth utilisation and errors;

   v) System and security log anomalies;

   vi) Successful access attempts, user account, date/time, session duration;

   vii) Unsuccessful access attempts;

   viii) Unusual network traffic.

b) Users of the company's data communications infrastructure, services, systems and applications may be monitored by company's authorized personnel without consent for legitimate purposes such as:-

   i) Recording evidence of transactions;

   ii) Policing regulatory compliance;

   iii) Detecting crime or unauthorized usage;

   iv) Safeguarding the integrity of the company's information communications technology infrastructure.

c) Use of sniffers to monitor network traffic and activity shall be allowed only for authorized Data Networks Telecommunications Engineers.

d) The company's network backbone infrastructure shall be monitored 24 hours a day, 7 days a week.

e) Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

12.4 Physical Access

12.4.1 Access Security to Server Rooms

a) Physical access to data centres and equipment rooms must be controlled using swipe cards, keypad controls or other electronic access control systems. Where locks with keys are used, procedures for secure management of the keys must be put in place.

b) Access to IT&T installation centers must be authorized and level of access given by the CM IT&T.

c) IT&T servers and telecommunication equipment shall be installed in dust free rooms, which have a high restriction means of access, highly reliable air-conditioning system and a fire security and alarm system. IT&T servers and telecommunication equipment should be mounted in such a way that it shall withstand minimum physical abuse.

d) Eating and drinking in the server room is prohibited.

e) Proper dress code shall be observed in the server room in-order to comply with the SHE requirements.

12.4.2 Access to PSC and SCADA Rooms, Cabinets and Network Equipment

a) Access to PSC rooms and SCADA/ SAS rooms located in substations and control centres shall require personnel to be certified by KPLC authorization committee as competent personnel with relevant authorization classes as per *KPLC Electrical Safety Rules 2011 Edition*.

b) All PSC and SCADA/ SAS rooms as well as RTU cabinets shall be locked at all times.

c) Unauthorized entry and access to PSC rooms and cabinets, and interference with PSC network equipment is strictly prohibited.

d) Other than in an emergency, access to communications rooms, cabinets and PSC network equipment shall be restricted to designated members of staff of the PSC section.

e) Access to communications rooms, RTU cabinets and PSC network equipment by third parties and contractors shall be under the supervision of an authorized designated member of IT&T Division.

12.5 Security of IT&T Hardware Assets

a) Users are responsible and accountable for the security of all IT&T hardware allocated to them either in office or out of the office.

b) All IT&T hardware should be clearly and permanently marked as belonging to KPLC and as indicated in the SATIS documentation.

c) Appropriate mode of transport sanctioned by the company that will ensure security of IT&T hardware shall be used for movement of equipment between work stations/depots/ offices/sub-stations.

d) Staff shall take appropriate care of all assets under their care/control. Damage caused to IT&T hardware as a result of negligence or careless handling may result in the staff being surcharged.

e) Laptops used in the office should be locked with the security lock when left unattended.

f) The IT&T inventory registry must be verified against the asset register with Finance department at least annually by CSA/CET.

12.6 System Security

a) Sectional and departmental heads should inform IT&T security on all new IT&T projects for the security team to perform risk analysis to identify new risks exposed to the current IT&T infrastructure by the new project and recommend mitigation measures. IT&T security should form part of the design team of any new IT&T project.

b) IT&T system security should conduct risk analysis on IT&T infrastructure annually and recommend mitigation measures.

c) Laptops should be encrypted using the approved encryption tool before being issued to users.

d) All IT&T user hardware and servers should be installed with the company's approved antivirus software. Users should ensure that their hardware is installed with the approved antivirus software and users should not uninstall the antivirus software.

e) Users are responsible for their system access accounts and are responsible for all the transactions and activities carried out on the KPLC IT&T systems using their accounts.

f) IT&T systems with connections to the public Internet should be placed behind the Network firewall in a DMZ network and assigned a NAT private IP. Access logs of these systems should be maintained and monitored to detect intrusion from the outside network.

g) Shared service accounts of all IT&T systems such as database accounts, router and switch accounts, administrator domain accounts should be changed on a regular basis where applicable.

h) Use of non KPLC IT&T user hardware and other portable devices to access Company systems or to perform company work should be authorized by CSA and details of the hardware registered.

13. VPN/MOBILE WORKER TECHNOLOGIES POLICY

a) It is the responsibility of the employee with VPN access to KPLC network to ensure no unauthorized user accesses KPLC network.

b) VPN access is controlled using username and password authentication as is contained in KPLC's active directory.

c) Users of this service are responsible for the procurement and cost associated with acquiring basic internet.

d) A user shall seek authority to use this service from the immediate supervisor who shall request for the provision of this service for the user from the CET/CSA.

e) Only authorised VPN client software shall be installed on users' laptops.

f) Logs for all network access via VPN/mobile worker technologies shall be kept in appropriate security devices such as the ACS server and Syslog Server.

14. TELEPHONES/FAXES/ VIDEO CONFERENCE SYSTEMS POLICY

14.1 Telephones/Faxes

a) Telephone or faxes shall be used for official business purpose only.

b) Users shall ensure restricted access to their phone facility through use of PIN that is only known to him/her.

c) Cost controls and/or new requests associated with use of phone facilities shall be implemented in line with HR (Administration) Policy through use of the telephony policy, appropriate call reporting and accounting software. Any abuse of usage should be reported to HR & ADMIN Department or to the Security Office.

14.2 Video Conference

a) All requests for use of video conference facility shall be sent to the CET/IT&T department at least one day prior to the meeting unless it is an emergency meeting.

b) Video conference equipment shall not be used unsupervised by the appropriate video conference system administrator.

c) No video conference session shall be recorded in any way or in any media without written permission of all individuals involved.

d) A log of all video conference sessions shall be kept by the relevant video conference system administrators.

15. IP ADDRESSING POLICY

a) IP address inventory clearly defining public and private IP address space, and allocating that address space to locations, subnets, devices, address pools, and users on the network shall be centrally kept and administered to maintain accuracy and consistency.

b) A record of what device is occupying what IP space in a subnet shall be kept by use of a central IP addressing manager.

c) Unused IP addresses shall be recovered as is appropriate.

d) Process for requesting IP address(es) shall involve submitting a case to the relevant data networks engineer. The following information shall be provided in the request:
   a) Subnet
   b) VLAN
   c) Current IP (If any)
   d) Port
   e) Protocol
   f) Any other useful information.

16. FIBER OPTIC CABLE ALLOCATION POLICY

a) Allocation of fiber optic cores within the KPLC fiber optic network for any functions shall be done on application to the CET.

b) The above shall apply for both internal and external prospective customers.

c) An updated log shall be kept of all fiber cores allocation countrywide including the core number.

d) In the case of relinquishing fiber cores, this shall also be updated in the master inventory log file.

e) Requests for tests on any cores on any link shall be made through the CET.

f) Access to any KPLC facilities to test or work on any fiber shall be done only on request to the relevant Functional Head and the work shall be carried out by or under the supervision of an authorised IT&T Officer.

17. DATA/DISASTER RECOVERY CENTRE POLICY

a) There shall be three levels of access to the Data/Disaster Recovery Centre: General Access, Escorted Access and Limited Access.

   i) *General Access* shall be granted to those who need free access authority to the data/disaster recovery centre on account of their job responsibilities e.g. server or telecommunications administrators.

   ii) *Escorted Access* shall be granted to people with legitimate business need to access the data/disaster recovery centre but infrequently. Such people include equipment contractors and installers, consultants, etc. They shall access the data/disaster recovery centre under direct supervision by someone with General Access. They shall sign in and out of the Data/Disaster Recovery Centre.

   iii) *Limited Access* shall be granted to a person who does not qualify for General Access but has legitimate reason for unsupervised access to the data/disaster recovery centre e.g. other telecommunications/IT support staff.

b) All doors to the Data Center must remain locked at all times and may only be temporarily opened for as minimal period as necessary in order to:

   i) Allow officially approved and logged entrance and exit of authorized individuals;

   ii) Permit the transfer of supplies/equipment as directly supervised by a person with General Access to the Data/Disaster Recovery Centre.

c) Prop open a door to the Data Centre ONLY if it is necessary to increase airflow into the Data Center in the case on an air conditioning failure. In this case, staff personnel with General Access must be present and limit access to the Data Center.

d) When an unauthorized person is found at the Data/Disaster Recovery Centre, it must be reported immediately to the manager in charge of IT or telecommunications.

18. IT&T TRAINING POLICY

a) Training shall be carried out in such a manner that all IT&T staff undergo continual capacity training so as to be up to date with market trends and technology.

b) Every section within IT&T division shall identify training needs every beginning of financial year and forward to the IT&T training co-ordinator through CM IT&T.

c) The training needs will be forwarded to HR training department to be included in the overall company training schedule.

19. PROCUREMENT POLICY

All procurements will be done in line with the *Public Procurement and Disposal Act (2005)* and the organisation's procurement rules.

Procurement of all IT&T systems shall remain the sole responsibility of the IT&T Division. Where other user Divisions require specialised IT systems, they shall forward all their requests to IT&T Division for determination to avoid duplications of systems and to ensure smooth after-purchase support.

19.1 Procurement of IT Systems

a) Procurement of user computers, laptops, printers should be based on the user requirement specification document that should be collected centrally by June of every year to CSA Central Office and approved by CM.

b) Technical specifications for the purchase of user computers, laptops and printers, servers, server applications, production printers and maintenance services should compiled in a RFQ document that should be approved by CSA.

c) Procurement of servers, server applications, production printers and maintenance services should be based on a Proposal/TC Paper that is approved by CSA.

d) A list of new IT&T hardware should also be presented to Insurance through CSA for insurance purposes.

19.2 Procurement of Telecommunication Hardware, PSC and SCADA Equipment

a) Design and procurement of network installations shall be planned and coordinated centrally by the CET.

b) Each section shall stock standard spares for network devices and installations to reduce down-time in case of failure.

c) No network hardware shall be procured without approval granted through a document approval form.

d) A decline or change in acquisition of a network hardware or installation by the authorizing officer(s) shall be provided through a brief as regarding the decision to the relevant telecommunications engineer.

e) In the case of need for PSC and SCADA equipment to be procured by a third party, for example as a part of a larger scope of work, IT&T Division shall be incorporated and involved from design stage to completion to be able to operating and maintaining the equipment. The request shall be through the CET.

20. TELECOMMUNICATION BUSINESS UNIT POLICY

20.1 Introduction

KPLC has an NFP license for selling dark fibre.

20.2 Policy Objectives

This Policy sets out rules and guidelines put in place by TBU department to realize KPLC's business objective of selling dark fibre and other associated facilities.

20.3 Scope

The Policy spells out the cross-functional issues of TBU related to the business of selling fibre. Keys areas covered in the Policy are issues dealing with customer identification and contracting, operations and maintenance (O&M), co-location of customers, and how to terminate services rendered to customer. The Policy does not delve in detail in matters related to contract negotiations and ADR settlements.

20.4 Third Party Contracting Policy

a) Third Party users are all parties that ride on KPLC's infrastructure to offer IT&T services to end users/customers. This includes those leasing KPLC fiber, KPLC premises for co-location and distribution network infrastructure to string third party fiber and coaxial connections for data, voice and cable television connectivity to end users/customers.

b) All such applications shall be channeled through the TBU Manager for approval and allocation of technical resource from KPLC to provide guidance to the third party user.

c) The Third Party users shall not be allowed access to KPLC infrastructure without the presence of an authorized KPLC IT&T representative.

d) Any work being carried out within the KPLC infrastructure by the third party user shall require the KPLC IT&T personnel to take the relevant authorization permits from within KPLC and sanction it with the relevant control centre as per SHE requirements.

e) The TBU Manager shall keep an active log of all third party connections within the KPLC infrastructure.

f) Requests from customers shall be sent to CRO who will issue prerequisite documents for fibre sell, and or co-location.

g) Customers are required to meet all legal and regulatory requirements as per the CCK requirements before approval to contract are accepted.

h) Terms and conditions forming the relations between KPLC and customers on lease of dark fibre and co-locations facilities are not negotiable and shall be based on approved terms and conditions by KPLC management and shall not have special conditions in favour of or otherwise to any customer.

i) Approvals shall be sought from the Company Secretary's office whenever contracting with external customers.

j) Denial of service to customers shall be communicated within 30 calendar days upon receipt of request.

20.5 Customer Support and Billing Policy (Service Delivery Policy)

a) SLAs shall be entered between KPLC and the customers detailing KPLC's support obligations and escalation levels.

b) A detailed feedback form on service delivery by KPLC shall be filled on quarterly basis by customers.

c) Customer billing and costing for services rendered by KPLC shall be non-discriminatory and shall be done on quarterly basis as per the contract terms.

d) Billing of customers shall be done based on the international accepted accounting best practice and standards.

e) Approvals must be sought from KPLC management for all tariffs applied in billing of customers.

f) Resource allocation (fibre pair, Shelter, cabinet, etc.) shall be done upon request and based on availability of that particular resource.

20.6 Customer Connectivity and Allocation of Other Resources Policy

a) Customer connection shall be done upon execution of contractual documents and payment of deposit as per the terms and condition of the contract.

b) Customers shall not be allowed to be connected to KPLC facility for more than 30 days effective from the date on the Conditional Certificate of Acceptance.

c) Site tests and ODF activations shall be conducted by both parties and an acceptance report shall bear evidence of parameters accepted by both parties.

d) Safety and access to KPLC rooms and substations where fibre equipment, and or cabinets are located shall be in-line with the SHE Policy.

e) All personnel requesting for access to such rooms and substations shall provide substantial proof that they have authority of the SHE department to access such premises.

20.7 Contract Execution, Management and Termination Policy

a) Fibre sell contracts shall be effected upon execution of the contract agreements by both parties and shall have commencement date which will be the date the service is activated.

b) Co-location and interconnect contract shall be drawn after the IRU/Lease main contracts have been executed for a particular route causing the co-location or interconnection and their terms and condition shall not be in conflict with the lease contract.

c) TBU Legal Officer shall maintain a database for contract status, routes, terms and conditions for all contracts.

d) Termination of services shall only be effected upon approval by TBU manager and upon such evidence proving non-compliance to contractual terms and conditions on the part of the customer, provided that where a customer requests for terminations on service by notice to KPLC, such termination shall not be denied unreasonably.

21. STATEMENT OF COMPLIANCE TO THE POLICY

a) The CM IT&T shall be responsible for enforcing these policies and taking appropriate action where there is non-compliance.

b) Failure to comply with these policies may result in any of the following actions being taken: –

   i) Cancellation or suspension of use of any IT&T facilities, systems or technologies

   ii) Payment for loss, damage or repairs

   iii) Civil or criminal liability under applicable laws

   iv) Disciplinary action under any other appropriate KPLC policies including suspension, expulsion or termination of employment

   v) Any other action that KPLC deems fit.

c) Where otherwise stated or approved, exceptions to this policy MUST have prior approval of the General Manager – IT & T (or equivalent) and if it is of material nature, the Board of Directors must ratify such changes.

22. REVISION

The Document will be revised as deemed necessary but its review shall be done in period sequence not exceeding two years.

23. APPROVAL

This IT&T Policy document in its initial form has received the following review and approvals from Kenya Power management:

Prepared By:
KPLC IT&T Policy Team

Signature & Date: _____

Checked By:
INFORMATION TECHNOLOGY MANAGER

Signature & Date: _____

Approved By:
GENERAL MANAGER, ICT

Signature & Date: _____

Approved By:
MD & CEO

Signature & Date: _____

www.kenyapower.co.ke customercare@kplc.co.ke Kenya Power
@kenyapower 95551 0703-070 707, 0732-170 170