DRAFT UTNWFT OPERATIONS MANUAL

Published by:

FOREWORD

The Trust, based on the principles of accountability and transparency, and the need to put in place systems that are efficient in financial accounting, procurement, human resources management, administrative services, office space accommodation and operational needs, intends to establish two offices, one at the headquarters located in Nairobi and the other will be in Sagana HCDD office compound in Sagana township, Kirinyaga County. This is to facilitate effective support to the operations of the Trust by bringing services closer to the customers and by also establishing accountable and transparent systems in all operations. In this regard, the Trust will avail adequate office space, for the staff, install and maintain up-to-date ICT equipment sans systems, servers, internet connectivity, suitable office equipment and working tools, furniture, and efficient transport system. The trust will also ensure adequate availability budget provision for all operations annually including rent, utilities, and other consumables.

Furthermore, the Trust, will also establish a governance structure and systems that embraces the corporate governance ideals. This will enable its management function to be effective and efficient thus facilitating achievement of the trust's goals and objectives. Key to this would be to build both institutional and technical capacity for effective operations of the trust. This is the main reason for developing this operational manual as a code of operations for the trust.

The creation and implementation of this manual is important to increase efficiency and accountability in the use and deployment of scarce resources. This manual provides a framework in which key information regarding service delivery and service arrangements are capture and documents in Upper Tana-Nairobi Water fund Trust. It outlines the context of the services, the service philosophy of care and gives a clear referral and assessment procedures.

The Executive Director will be responsible for implementing this operational manual with full compliance to the trust deed, laws, rules, and regulations. The BoT will support the implementation of the manual through regular policy briefs and directives while the BoM will provide the oversight support to its implementation. Nevertheless, the Board of Trustees (BoT) is committed to full implementation of all provisions of this manual

for the trust to deliver on all expected outcomes as desired. I therefore call upon the trust management to fully adhere to the provisions of the manual in all operational areas.

Emmanuel Rurema
Chairman, UTNWFT

TABLE CONTENTS

DEFINITIONS AND ABBREVIATIONS

UTNWF	Upper Tana-Nairobi Water Fund
TNC	The Nature Conservancy
ACS	Access Control Server
ADR	Alternative Dispute Resolution
CET	Chief Engineer Telecoms
CM	Chief Manager
CPU	Central Processing Unit
CSA	Chief Systems Analyst
HR	Human Resource
IT	Information Technology
ICT	Information and Communication Technology
IP	Internet Protocol
IRU	Indefeasible Right of Use
IT	Information Technology
LAN	Local Area Network
NAT	Network Address Translation
NFP	Network Facility Provider
NMS	Network Management System
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private network
Contractor	Any person engaged to provide a specific service or goods.
Hardware	The physical aspect of computers, telecommunications etc
User	Any person authorized to use IT facilities or systems.

CHAPTER 1

1. INTRODUCTION

1.1. About Upper Tana-Nairobi Water Fund (UTNWF)

The Upper Tana-Nairobi Water Fund Trust (UTNWFT) was established in October 2015 and incorporated in October 2017 as a charitable Trust in Kenya with a mission to secure the long-term conservation, protection and maintenance of the Upper Tana Watershed and the benefits it provides for people and nature by advancing nature-based solutions to water security. UTNWFT is an international non-governmental organization established by The Nature Conservancy (TNC) in collaboration with the government and has its headquarters in Nairobi, Kenya.

The organizational structure of the trust has two operational levels of governance and management comprising of the Board of Trustees (BoT) at the apex whose mandate is to set Policy Direction, Vision and Mission of the trust; The Board of Management (BoM) whose mandate is to oversee the overall implementation of the trust programmes, projects and activities in a coordinated manner operating at the trust headquarters; The County Advisory Committee (CAC) whose responsibility include mainstreaming county policies into the water fund implementation framework for smooth water fund activities implementation; re-aligning their activities as the co-funders of the water fund activities by providing subsidies and a team of top managers comprising of professional staff whose functions is to oversee day to day operations of the trust.

The operational components of the Trust include:

i. Hiring of well skilled and experienced staff
ii. Well set up office space and equipment
iii. Vehicle resources
iv. Two well fitted office facilities and
v. Functional databases for storing conservation information, monitoring equipment and a host of other resources necessary for day-to-day work.

1.2. About the Manual

This document provides a framework in which key information regarding service delivery and service arrangements are captured and documented for Upper Tana-Nairobi Water Fund Trust. It outlines the context of the services, the service philosophy of care and gives a clear referral and assessment procedures.

The Manual shall be reviewed regularly and at least every three years. The review shall be an inclusive process that involves the Finance Manager(s) and approved consultant(s). All users are requested however to send any comments they may have as and when they come up to the Senior Management /Executive Director. After review with interested parties, any necessary amendments shall be authorized and distributed by the Executive Director. The amendments shall be distributed initially to the Board of Directors and Finance Managers, who shall in turn distribute them to all finance staff or other users in their area of responsibility.

The Finance and Administration Manager is responsible for making the Manual easily available to Management, Project, and Finance staff. The Finance Managers shall ensure that their copies of this manual are kept up to date with current Policies and Procedures.

CHAPTER 2

2. OFFICE SPACE MANAGEMENT

This policy provides the framework for the management of office space. It recognises that the needs of individual staff shall vary depending on their particular role. The policy takes full account of the organizational priorities.

2.1. General facilities management procedures

This policy will be implemented by the Administration and Finance Officer. The management of Upper Tana-Nairobi Water Fund Trust shall ensure that there is space for use and management of the organizational activities. The following general procedures shall apply:

i. Office space shall be allocated for use by staff by the management. There shall be no specified time limit to allocations although some are made to meet temporary needs. Allocations may be subject to review and Upper Tana-Nairobi Water Fund reserves the right to reallocate space in response to changing needs and priorities, while seeking to do so with the agreement of staff affected.
ii. Office allocations shall be made by the administration department.
iii. Applications to make office changes must be presented to department and in sufficient time to allow authorisation and action by the various professional services involved.
iv. The finance and administration department will seek to maximise the effective use of office space and to ensure that space needs are met appropriately. Members of staff should not have more than one office. Members of staff shall not be allocated an office without windows.
v. Upper Tana-Nairobi Water Fund Trust shall provide mobile technology and other support staff who do not wish to have an office space allocation. It is expected that all established staff will be provided with office space appropriate to their needs.
vi. Where appropriate, accommodation for infrequent users of office space will be provided with agreement by utilising hot desk areas when available.

vii. Part-time staff and visiting professors will normally be located in shared office space.

viii. Workrooms should have enough free space to allow people to get to and from workstations and to move within the room, with ease. The number of people who may work in any particular room at any one time will depend not only on the size of the room, but on the space taken up by furniture, fittings, equipment, and on the layout of the room. Workrooms, except those where people only work for short periods, should be of sufficient height (from floor to ceiling) over most of the room to enable safe access to workstations.

2.2. Furniture Provision

Space permitting, the standard furniture per person for an office shall be:

i. 1 Desk
ii. 1 Pedestal or set of desks draws.
iii. 1 Fit for purpose operator's chair
iv. Bookcases, as appropriate
v. Guest chairs, as appropriate
vi. 1 Pin board
vii. 1 Whiteboard
viii. 1 Desk lamp

All other furniture requests are considered on a case-by-case basis. Where stock furniture is available additional items may be supplied from stock. Departments shall be required to purchase additional non-standard items through the procurement department. The Finance and Administration department shall provide pin and white boards on request. Office users are not permitted to attach items to walls in anything other than frames or pin boards. The use of unauthorised electrical equipment in offices shall not be permitted, such as fridges, chilling cabinets, microwaves, kettles, toasters, heaters, air conditioning units. Office users are responsible for the electrical safety use of any non-Upper Tana-Nairobi Water Fund equipment.

2.3. Lease agreement

The board shall be the sole body responsible for acting on behalf of the organization in binding contractual agreements. The Executive Director and the chair of the Board shall append their signatures to such documents or agreements as consent to enter into such agreements.

CHAPTER 3

3. VEHICLE MANAGEMENT

The Finance and Administration Officer is responsible for the implementation of this policy.

These policies for vehicle management apply to the provision, use, control, insurance, maintenance, safety and protection, accidents, and theft of UTNWFT owned and controlled vehicles.

3.1. General Guidelines for Use of Vehicles for the UTNWF Office

The use of UTNWFT office vehicles must always serve the best interests of UTNWF. The following rules apply:

i. In principle, vehicles will be used only for official UTNWF business.

ii. Vehicles must be kept in good working condition to minimise repair and maintenance costs and to maximise the resale value.

iii. Safety and security guidelines are strictly followed.

iv. Only authorised persons holding a driver's license valid in the duty station may drive the car.

v. In using UTNWFT vehicles, the maximum overtime allowed for drivers must be respected. In the interests of the health of the staff and the efficiency of the service, a staff member should not be required to work more than 40 hours of overtime during any one month, except where unusual exigencies of the service so require. If more than one driver works for UTNWFT, and if the overtime hours of the driver concerned relate to official business, then the supervisor should distribute the overtime hours equally among them.

vi. When not in use, vehicles are to be parked in a safe area designated by the UTNWFT executive director, UTNWFT representative, chief of operations, chief of liaison office or UTNWFT representative.

vii. The vehicle fuel tank must be filled completely at each refuelling so that the fuel consumption rate may be verified. Where petrol coupons are in use, a register must be maintained for petrol coupons providing data on acquisition and use and the data must reconcile with vehicle records. Coupons must be stored in a safe place and their use must be controlled by administrative staff.

3.2. Driver Safety Policy

All drivers are expected to abide by the following:

i. **Safety Belts:** The driver and all occupants are required to wear safety belts when the vehicle is in operation or while riding in a vehicle. The driver is responsible for ensuring passengers wear their safety belts.

ii. **Impaired Driving:** The driver must not operate a vehicle at any time when impaired, affected, influenced by alcohol, illegal drugs, prescribed or over-the-counter medication, illness, fatigue, or injury.

iii. **Traffic Laws:** Drivers must abide by the government local motor vehicle regulations, laws, and ordinances.

iv. **Vehicle Condition:** Drivers are responsible for ensuring the vehicle is maintained in safe driving condition.

v. **Cellular Telephones, Electronics:** Drivers who wish to use cellular telephones must have an external speaker and microphone to allow hands-free operation and locate a safe location to stop the vehicle to place/take a call or text. Employees are prohibited from using any type of MP3 player or similar device with earphones while operating a motor vehicle.

vi. **General Safety Rules:** Employees are not permitted to:
    a. Smoke while operating the motor vehicle,
    b. Pick up hitchhikers,
    c. Accept payment for carrying passengers or materials,
    d. Use any radar detector, laser detector or similar devices,
    e. Assist disabled motorists or accident victims beyond their level of medical expertise. If a driver is unable to provide the proper medical care, he/she must restrict his/her assistance to calling the proper authorities. The driver's safety and wellbeing is to be always protected.

vii. **Fund and Personal Property:** Employees are responsible for UTNWFT property such as computers, work papers and equipment under their control. UTNWFT will not reimburse the employee for stolen personal property.

3.3. Insurance Coverage

The management of UTNWTF shall ensure that all vehicle both owned by the Fund and those provided by third parties for various projects are adequately insured.

CHAPTER 4

4. FIXED ASSETS MANAGEMENT

The Finance and Administration Officer is responsible for the implementation of this policy. Assets which are capitalized are considered fixed assets and are recorded in the fixed assets section of the general ledger and in the fixed assets register. Fixed assets can either be acquired by gift or by purchase. The assets (assets owned by a project donor) shall not be accounted for within Upper Tana-Nairobi Water Fund Trust books of account. Transfer of any Trust fixed assets to any other entity shall be as per an agreement or MoUs developed and approved by the parties involved.

4.1. Fixed assets capitalization

A fixed asset is any moveable/tangible or intangible asset with a useful life of more than one year.

4.2. Fixed Assets Policy

i. Project assets shall be fully expensed as project expenditure on acquisition.
ii. The asset cost includes all costs directly attributable to bringing the assets to their intended working condition such as purchase cost, taxation, transportation, and installation.
iii. The responsibility for approving purchases of Upper Tana-Nairobi Water Fund Trust owned assets lies with the Executive Director.
iv. The acceptance of donated assets must be approved by the Executive Director who in consultation with the Finance Manager shall determine the value of the assets which shall include all associated costs.
v. Consideration must be given to determine the economic feasibility of accepting and maintaining donated second-hand assets before accepting them. However, if there are costs to be incurred in accepting the asset, approval must be obtained based on the existing approval matrix.
vi. All fixed assets shall be under the overall custody of the individual staff to whom they are assigned to in the system and in the relevant location. The user shall be responsible for keeping asset in good condition and secure.

4.3. Fixed Asset Acquisition

Assets either owned by Upper Tana-Nairobi Water Fund Trust or by individual projects (*project assets*) can be acquired through gifts or direct purchase.

i. The purchase of all assets shall be as per the approved guidelines or specification as issued by Upper Tana-Nairobi Water Fund Trust from time to time.
ii. The Upper Tana-Nairobi Water Fund Trust procurement procedures shall apply in the purchase of fixed assets.
iii. Upon receipt of the assets, the user department must confirm that all the assets have been delivered and are of approved quality and quantity.
iv. For all assets purchased, the Cost Centre Manager shall ensure that a warranty is received where applicable.

4.4. Transfer of movable assets

i. Moveable assets may be transferred from one location to another as necessary for operational purposes.
ii. The authority to transfer the asset shall be given by the Executive Director following which an Asset Transfer Form must be completed.
iii. Project's assets shall be transferred as stipulated in the signed agreement between Upper Tana-Nairobi Water Fund Trust and the donor.
iv. Each project shall maintain an asset register which shall be updated regularly.
v. The asset shall be delivered to the location where it is needed together with the transfer form. The form shall be signed by the person receiving the asset and returned to the respective department/programmes for re-allocation and the amendment of the Fixed Assets Register.

4.5. Managing Fixed Assets

i. The Administrative Officer shall allocate a number to the assets, tag the assets and all the relevant details shall be maintained by the Financial Accountant who updates the General Ledger and Fixed Assets Register.

ii. Project assets are fully expensed as project expenditure at the time of purchase and are not capitalized. The head quarters assets are capitalized on acquisition.

iii. Fixed assets shall be managed on a day-to-day basis by the assigned users who are responsible for the security and maintenance of the relevant asset.

4.6. Safeguarding Fixed Assets

i. Use of all Upper Tana-Nairobi Water Fund Trust assets shall be restricted to only the authorized activities and persons.

ii. All assets shall be maintained in an appropriate secured area where access is restricted to authorized personnel.

iii. Assets shall be insured, and the value of insurance shall be determined by the officer in charge for insurance. The insurable value shall be the replacement value and not the purchase price.

iv. For insurance purposes the value of the assets shall as much as possible be the market value and reviewed regularly. Any asset that is not in a good condition must be reported by the assigned user to the Administrative Officer for immediate action.

4.7. Maintenance of fixed assets

i. Upper Tana-Nairobi Water Fund Trust shall follow the recommended manufacturer schedule for maintenance and all assets shall be maintained in good working conditions.

ii. The Administrative Manager shall review the costs for maintenance to ensure that the maintenance costs are economic and reasonable for the asset.

4.8. Year-end procedure for fixed assets

i. A physical verification exercise shall be carried out at least once a year for fixed assets with high risk and high value both at field offices and the HQ level. This shall be done by the Administration office. Other assets shall be verified at least once every two years.

ii. The physical verification shall then be reconciled with the field asset register for confirmation purposes.

iii. The respective accountant shall update the fixed assets register at the end of each financial year in accordance with IFRS having reconciled the physical verification with the fixed assets register and the general ledger. This shall be reviewed by the Administration and Finance Officer.

4.9. Title Documents

i. All title documents shall be kept by the Secretary and copies maintained by the Executive Director.
ii. The title documents must be kept under lock and key and equipment that ensure high levels of safety i.e., fireproof cabinets and the use if safety deposits.
iii. No title documents shall be used as security for any borrowing unless with the approval of the Board of Directors. Where the assets have been financed by the donor the approval must be sort from the donor unless the assets have already been transferred to Upper Tana-Nairobi Water Fund Trust.

4.10. Fixed Asset Depreciation Policy

i. Depreciation is charged annually on a straight-line basis to write down the cost of each asset to its residual value over its estimated useful life. Where monthly/quarterly reporting is a requirement, depreciation shall be apportioned as such.
ii. On all assets purchased or disposed of during the year, depreciation is charged prorate.
iii. Depreciation shall be calculated at least monthly based on the management policy or wear and tear KRA policy by the designated Project/Programme Accountant.
iv. Journals to charge the depreciation cost to the relevant expenditure account shall be run at least quarterly so as to update the periodic depreciation charge and accumulated depreciation accounts in the general ledger.

4.11. Fixed Assets Disposals

i. For disposal of assets, the Cost Centre Manager shall prepare a schedule of items that are due for disposal in consultation with the Administration

Manager then advice the Executive Director who shall approve according to their limit of authority.

ii. Disposal of Upper Tana-Nairobi Water Fund Trust assets must be approved by the (BoT) as stipulated in the procurement policy.

iii. Where appropriate, an independent valuation shall be obtained from a valuation expert disposal to help establish market value.

iv. Upper Tana-Nairobi Water Fund Trust shall ensure that where applicable, payment of all the government duty is made before disposal of any asset.

4.12. Revaluation of Fixed Assets

i. Any revaluation of Upper Tana-Nairobi Water Fund Trust fixed assets shall be carried out by professional valuers. The revaluation date shall coincide with the year-end date of 31st December.

ii. In the year of valuation, the financial statements shall disclose the basis of valuation together with the name and qualifications of the valuer.

iii. If after a revaluation exercise the value of a certain asset is below the net book value, the difference shall be written off against the reserve account.

iv. The revaluation reserve is not available for distribution unless the revalued asset is sold.

v. On disposal of a previously revalued asset, the related balance of accumulated asset reserve shall be transferred to Income and Expenditure Account.

4.13. Project Assets

4.13.1. Project Assets Policy

i. Project assets purchased for use during the project, under the management of Upper Tana-Nairobi Water Fund Trust but owned by a third party. The ultimate ownership of the asset is dependent on the contract agreement or a decision to be made by the donor at the end of the project.

ii. All project assets are expensed immediately on acquisition and charged to the appropriate project cost centre.

iii. The Finance Manager shall ensure that records of all project assets are properly maintained, and assets therein are physically present.

iv. The HQ shall maintain a fixed asset listing detailing the relevant details of Project Assets.

v. Any disposal/transfer of a project asset must be approved by the Executive Director or the Board according to the donor contract and Upper Tana-Nairobi Water Fund Trust procedures for disposal.

vi. From time-to-time the Finance Manager shall ensure that a verification process is conducted to confirm that the project assets listed are physically in existence and confirm the physical condition and location of the asset.

4.13.2. Project Assets Procedure

i. Project Assets shall be acquired using the Upper Tana-Nairobi Water Fund Trust Procurement procedure and must comply with set standards.

ii. The cost of the asset shall include all related costs incurred up to the point when the asset is deemed operational; this shall include all the accessories, the freight and installation costs.

4.13.3. Donated Assets

From time-to-time Upper Tana-Nairobi Water Fund Trust may receive donations of assets to be used in a project. To be able to capture the full value of the asset into its accounts, Upper Tana-Nairobi Water Fund Trust shall capitalize the asset at the value advised by the donating agency. The value of the assets shall include all the transportation and installation costs.

CHAPTER 5

5. ICT MANAGEMENT POLICY

5.1. Statement of Purpose

The Finance and Administration Officer is responsible for the implementation of this policy. This Policy section serves as a guide to the users of IT facilities and equipment and prescribes the boundaries within which decisions can be made. The objectives are:

i. Ensure minimization of risk in the use of IT facilities and equipment and to indicate mitigating methods where risks exist.
ii. Ensure implementation of security requirements in the use of IT facilities and equipment.
iii. Provide users with standards to abide by.
iv. Provide a framework for development, management and control of the various IT networks and systems.
v. Ensure compliance with the necessary statutes, regulations, and mandates in the running of every section of the IT Division.
vi. Uphold the image and integrity of the company through use of the defined standards and guidelines.

5.2. Scope of the IT Policy

This Policy applies to all Upper Tana-Nairobi Water Fund Trust stakeholders that use the Fund's IT facilities. These include any person that may access, develop, implement, test, commission and use any IT based information owned, managed, supported, or operated by, or on behalf of Upper Tana-Nairobi Water Fund Trust. Hence, all employees, contractors engaged by the company to carry out projects, develop, repair, or maintain the IT resources, suppliers of IT resources and customers shall comply with the policies stipulated in this document.

5.3. IT HARDWARE POLICY

5.3.1. New Hardware

Users shall be issued with an Assignment Note, which they shall sign upon receipt of every IT hardware i.e., rugged laptop, tablets, workstations, laptop, personal computer, printer and scanner, IP Phone, Blackberry, iPad, portable radios and mobile radios. 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. 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 Administration and Finance Officer
   - IT support staff shall verify the need for user hardware replacement or disposal.
   - All the recommendation for user hardware replacement or disposal shall be forwarded to Administration and Finance Officer.

ii. Rugged laptops, tablets, workstations, and other specialized user IT Hardware will be issued to employees upon request to IT Manager through Heads of Departments.

iii. IP Phones, portable/mobile radios will be issued to all levels of employees upon request to Administration and Finance Officer through the user's immediate supervisor.

5.3.2. Returning Hardware

Users shall be issued with a receipt note, which shall be signed upon returning any issued IT hardware.

5.3.3. Hardware Movement

i. Users shall be issued with a gate-pass during inter-branch movement of any IT hardware.

ii. Any IT equipment leaving any office facility for either repair or being carried away by a third party or contractor shall be issued with a gate-pass.

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

5.3.4. Lost Hardware

i. Users shall report any lost hardware to IT. User should present their signed Assignment Note to the Administration and Finance Officer 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 HQ office.
ii. The procurement shall provide procurement information on the lost item i.e., invoice number, purchase order to the Insurance Office for purposes of reimbursement.
iii. User may be surcharged for the lost item either fully or partially depending on the circumstances leading to the loss.

5.3.5. Inventory Control

i. All new hardware shall be entered into the system, which is the Assets Management System.
ii. A stock take shall be conducted every month of June in the financial year by IT Advisory.

5.3.6. Retirement of Obsolete IT Hardware Policy

i. 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.
ii. 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.
iii. IT 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.
iv. Obsolete IT hardware will be disposed of as per the following guidelines:

a. For disposal of assets, the IT Advisory shall prepare a schedule of items that are due for deposal in consultation with the Administration and Finance Manager then advice the Executive Director who shall approve according to their limit of authority.
b. Disposal of Upper Tana-Nairobi Water Fund assets must be approved by the board as stipulated in the procurement policy.
c. Where appropriate, an independent valuation from an expert shall be obtained before disposal to help establish market value.
d. Upper Tana-Nairobi Water Fund shall ensure that where applicable, payment of all the government duty is made before disposal of any asset.

5.3.7. Contractor Management Policy

i. A Service Level Agreement describing the services to be offered, performance measurement, incident management, suppliers and company, and the rules of engagement between the suppliers offering the IT services to be signed by the supplier and the Administration and Finance Officer.
ii. A Scope of Work document describing tasks to be completed by a supplier in an IT project, the location of work, period of performance, deliverable schedules, and acceptance criteria to be signed by the supplier and the Administration and Finance Officer before commencement of any IT project.
iii. 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 Administration and Finance Officer.
iv. Department/section heads responsible for contractors should request for user creation on company systems for the authorized contractors to access company systems.
v. Authorized contractors' computers should have minimum technical hardware and software specifications approved by Administration and Finance Officer.
vi. Different user accounts convention and user access matrix should be formulated for contractors.

vii. Authorised contractors working on IT equipment shall sign a non-Disclosure document.

5.3.8. Systems Backup

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. The total recovery time, after loss of data, consists of the time necessary for:
    a. Analysing the error.

b. Replacing the required hardware and setting up the operating system and required file systems.
c. Restoring the database from data backups.
d. Performing a forward recovery from backed up redo log files.
e. Performing an instance recovery automatically at system start-up.

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

ix. 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.

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

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

CHAPTER 6

6. MAINTENANCE POLICY

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

6.1. General Maintenance Policy

i. IT teams will schedule any planned systems maintenance at a time which has the lowest impact on the trust. They will be scheduled outside the normal company hours of operation.
ii. 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.
iii. Clients/customer representatives and other impacted stakeholders shall be notified when the required maintenance is completed, and system operations have been restored.
iv. Appropriate system maintenance logs and documentation shall be updated and reviewed after every maintenance.
v. IT personnel shall carry out scheduled maintenance as per the maintenance program approved and circulated by the Administration and Finance Officer.
vi. Breakdown maintenance shall be carried out as per the norms and procedures outlined in the IT Norms and Procedures.

6.2. Preventive Maintenance Policy

i. Preventive maintenance for user computers and printers shall be conducted twice yearly.
ii. 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.

iii. Contractors as per existing SLA/contracts shall carry out other Preventive Maintenances.

6.3. Comprehensive Maintenance Policy

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

Maintenance Policy on user hardware will be guided by the following:

i. Only IT 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.
ii. Installation manuals and media must be kept and readily available to the staff that are authorised to support or maintain systems.
iii. Only authorised and licensed software will be installed on hardware.

Maintenance Policy on software will be guided by the following:

i. IT Advisory shall advise on system upgrades.
ii. Systems software will be regularly maintained to ensure they meet the changing requirements of the various divisions and changes in technology.
iii. 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.
iv. For internal developments, a change request/ transport request form must be filled, and it must be duly signed for the change to be affected.
v. For systems maintained by contractors, a Service Level Agreement must be maintained, and any maintenance will be carried as per the Service Level Agreement.

CHAPTER 7

7. INCIDENT MANAGEMENT AND RESOLUTION POLICY

Incidences on IT hardware shall be managed guided by the following:

i. Management of incidences will be guided by the procedures in the IT Norms and Procedures document procedure for IT hardware.
ii. All IT user incidences shall be logged in the IT service desk system. In cases where users have trouble, the incidences should be reported through the support desk extensions, or through the respective regional support help, desk email addresses.
iii. Head of support shall distribute the support desk incidences and ensure that each incidence is resolved within the set resolution time.
iv. Users to be sufficiently informed of the IT service catalogue and escalation matrix for each service.
v. System incidences to be reported and resolved as indicated in the IT Norms and Procedures.

Incidences on portable and mobile VHF radios shall be managed guided by the following:

i. Radio equipment and communication failure shall be reported to the Administration and Finance Officer for allocation to IT resource personnel for troubleshooting and resolution.
ii. During troubleshooting 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.
iii. Radio shall be assigned to the user and the old one recovered.
iv. No external radio shall be configured for use within the company radio network.

CHAPTER 8

8. USER ACCOUNT MANAGEMENT POLICY

i. Supervisors should formally make requests for user account creation for their staff to the relevant IT section head for approval.

ii. All user accounts must be uniquely created.

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

iv. Users shall be granted privileges that are commensurate with their roles and responsibilities in the IT systems.

CHAPTER 9

9. 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. The following policy guidelines shall apply:

i. Departments must submit to a list of administrative contacts for their systems that are connected to the company's network.
ii. All user of administrative/special access accounts must have account management instructions, documentation, training, and authorization.
iii. Everyone that uses administrative/special access accounts must refrain from abuse of privilege.
iv. 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).
v. Each account used for administrative/special access must meet the Kenya Power Password Policy.
vi. 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.
vii. 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 via use of securely kept password envelopes.
viii. 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 and removed when work is complete.

ix. All non-users (under item viii must sign a Non-Disclosure Agreement (NDA) before account access is enabled.

CHAPTER 10

10. PASSWORD POLICY

Upper Tana-Nairobi Water Fund Trust passwords management shall be guided as follows:

i. Automated information systems to uniquely, identify individual users.
ii. Be at least six characters in length.
iii. Password complexity design shall be incorporated in all IT systems to include at least two of the following: upper case, lower case, special characters, and numbers.
iv. 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 systems.
v. 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.
vi. Passwords shall expire after every 30 days.
vii. Not be dictionary words.
viii. Not be portions of associated account names (e.g., user ID, log-in name, personal information).
ix. Not be simple keyboard patterns (e.g., QWERTY, asdf).
x. In addition, users are required to select a new password immediately after their initial log in.
xi. Users are responsible for the security of their password(s) and are accountable for any misuse.
xii. Incidents where a user suspects that his/ her accounts has been compromised shall immediately be reported to the IT Security.
xiii. Any default passwords must be changed on all systems prior to connection to any network, even in pre-deployment testing.
xiv. Screen-saver password must be enabled after 5 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.
xv. 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.

CHAPTER 11

11. INTERNET POLICY

i. Heads of departments shall formally request for internet rights for their staff to the CSA for approval.

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

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

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

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

vi. 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.

CHAPTER 12

12. EMAIL POLICY

i. Supervisors shall request company e-mail for their staff with approval from the IT Advisory.

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

iii. User should not reply to unsolicited e-mails received to company email address as this could allow the sender to verify addresses for purposes of sending a virus or hacking in the system.

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

v. Monitor the use and content of any email generated, stored and/or handled on its systems for detecting malware, spam, and viruses.

vi. Monitoring 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, security, or audit department.

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

viii. Email systems are principally provided for business purposes.

CHAPTER 13

13. ACCESS AND SECURITY POLICY

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

13.1 Network Access

i. Domain Controller/Active Directory shall control all access to network (via wired, wireless & VPN).
ii. Temporary/guest access shall be facilitated on request to IT Advisory.
iii. The guest on approval by the IT Advisory shall activate a guest account with appropriate permissions, with automatic date and time of expiry for temporary use.
iv. On resignation/termination of employment, employees will have their network access terminated during the clearing process.

13.2 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 Upper Tana-Nairobi Water Fund Trust's data communications infrastructure, services, systems, and applications may be monitored by Upper Tana-Nairobi Water Fund Trust'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 IT infrastructure.

c) Use of sniffers to monitor network traffic and activity shall be allowed only for authorized data networks telecommunications engineers.
d) Upper Tana-Nairobi Water Fund Trust's network backbone infrastructure shall be monitored 24 hours a day, 7 days a week.
e) Electronic logs that are created because of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

13.3 Physical Access

Access security to server rooms shall be guided by the following:

i. 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.
ii. Access to IT installation centres must be authorized and level of access given by the IT Advisory.
iii. IT servers and telecommunication equipment shall be installed in dust free rooms, which have a high restriction means of access, exceptionally reliable air-conditioning system and a fire security and alarm system. IT servers and telecommunication equipment should be mounted in such a way that it shall withstand minimum physical abuse.
iv. Eating and drinking in the server room is prohibited.
v. Proper dress code shall be observed in the server room in-order to comply with the SHE requirements.

Security of IT Hardware Assets

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

ii. All IT hardware should mark clearly as belonging to Upper Tana-Nairobi Water Fund Trust and as indicated in the system documentation.

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

iv. Staff shall take appropriate care of all assets under their care/control. Damage caused to IT hardware because of negligence or careless handling may result in the staff being surcharged.

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

vi. The IT inventory registry must be verified against the asset register with Finance department at least annually by Administration and Finance Officer.

System Security

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

ii. IT system security should conduct risk analysis on IT infrastructure annually and recommend mitigation measures.

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

iv. All IT 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.

v. Users are responsible for their system access accounts and are responsible for all the transactions and activities carried out on the IT systems using their accounts.

vi. IT 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.

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

viii. Use of non-IT user hardware and other portable devices to access company systems or to perform company work should be authorized by Administration and Finance Officer and details of the hardware registered.

CHAPTER 14

14. VPN/MOBILE WORKER TECHNOLOGIES POLICY

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

ii. VPN access is controlled using username and password authentication as is contained in active directory.

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

iv. 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 Administration and Finance Officer.

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

vi. 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.

CHAPTER 15

15. TELEPHONES/FAXES/VIDEO CONFERENCE SYSTEMS POLICY

15.1. Telephones/Faxes

i. Telephone or faxes shall be used for official business purpose only.
ii. Users shall ensure restricted access to their phone facility through use of PIN that is only known to him/her.
iii. 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 Administration and Finance Officer and or Security Officer.

15.2. Online meetings

i. All requests for use of video conference facility shall be sent to the IT Advisory at least five days before it is required. This request shall be authorised depending on the traffic. prior to the meeting unless it is an emergency meeting.
ii. Video conference equipment shall not be used unsupervised by the appropriate video conference system administrator.
iii. No video conference session shall be recorded in any way or in any media without written permission of all individuals involved.
iv. The relevant video conference system administrators shall keep a log of all video conference sessions.
v. Zoom or other applicable platforms for meetings shall also be adopted.

15.3. IP ADDRESSING POLICY

i. 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 kept centrally and administered to maintain accuracy and consistency.

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

iii. Unused IP addresses shall be recovered as is appropriate.

iv. Process for requesting IP address(s) shall involve submitting a case to IT Advisory. The following information shall be provided in the request: Subnet, VLAN, Current IP (If any), Port, Protocol, and any other useful information.

CHAPTER 16

16. DATA/DISASTER RECOVERY 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 Centre must always remain locked and may only be temporarily opened for as minimal period as necessary 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 Centre 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 Centre.
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.

CHAPTER 17

17. PROCUREMENT POLICY

The Finance and Administration Officer is responsible for the implementation of this policy. All procurements will be done in line with Upper Tana-Nairobi Water Fund Trust's procurement rules. Procurement of all IT systems shall remain the sole responsibility of the IT Advisory. Where other user HODs require specialised IT systems, they shall forward all their requests to IT Advisory for determination to avoid duplications of systems and to ensure smooth after-purchase support. The following guidelines will be followed for procurement:

i. Procurement of user computers, laptops, printers should be based on the user requirement document that should be collected centrally by June of every year to Administration and Finance Officer and approved by IT Advisory.
ii. Technical specifications for the purchase of user computers, laptops and printers, servers, server applications, production printers and maintenance services should compile in a Request for Quotes (RFQ) document that should be approved by CSA.
iii. Procurement of servers, server applications, production printers and maintenance services should be based on a proposal/TC paper that is approved by CSA.
iv. A list of new IT hardware should also be presented to insurance through Administration and Finance Officer for insurance purposes e.g., procured IT equipment.