NATIONAL WATER HARVESTING & HARVESTING AUTHORITY

Standard Operating Procedure for

ICT Management
NWHSA/FCP/SOP/04

Document Review Sheet

This Standard Operating Procedure will be reviewed from time to time.

1.0 AMENDMENT RECORD

This Standard Operating Procedure is reviewed regularly to ensure relevance to the systems and process that it defines. A record of contextual additions or omissions is given below.

Amendment Record Sheet

Amendment Date	Issue No.	Revision No.	Page No.	Subject Of Review /Modification	Revised By	Reviewed & Approved By

2.0 GENERAL

2.1 Purpose

To ensure that the proper database backup and recovery procedures are in place for all NWHSA data.

2.2 Scope

This procedure applies to and defines all activities carried out by the ICT Division.

2.3 References

- ICT Strategy

2.4 List of abbreviations

NWHSA	-	National Water Harvesting & Storage Authority
CEO	-	Chief Executive Officer
GM	-	General Manager
ICT	-	Information and Communication Technology
ICTA	-	ICT Authority

2.5 Definition of Terms

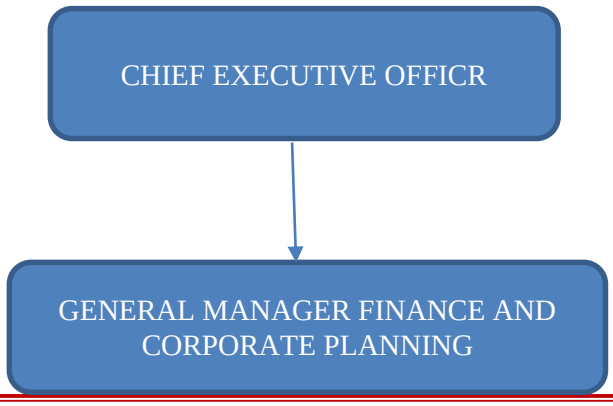
Accounting Officer	:	The Officer in charge of the Authority
Users	:	The Staff of NWHSA
Equipment	:	Refers to all ICT machines, laptops, desk tops, printers, servers, photocopiers

2.6 Responsibility

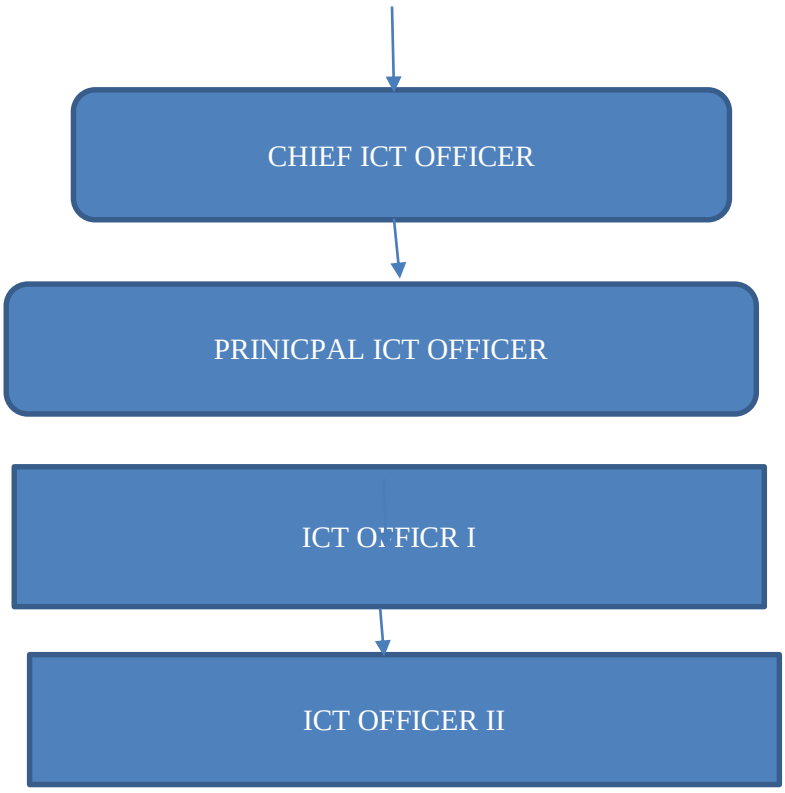
The Head of ICT Division has the primary responsibility of ensuring that these processes are implemented and remain adequate for their intended purpose. The Head has to provide the information from which documentation of the processes and activities can be compiled and for initiating action to keep them up to date. However, all divisional staff members are responsible for implementing and ensuring that these procedures are followed.

3.0 ADMINISTRATIVE STRUCTURE

The current administrative structure for the ICT Division is as follows:



U


CHIEF ICT OFFICER
PRINICPAL ICT OFFICER
ICT OFFICR I
ICT OFFICER II

4.0 PROCESSES

4.1 Overview

The ICT division is responsible for ensuring that the ICT equipment and data are properly kept and maintained for all NWHSA departments. The procedures are as follows:

(i) Database backup and archiving
(ii) Database recovery
(iii) ICT equipment maintenance

4.2 Process for Database backup and archiving NWHSA/FCP/SOP/04/DB

4.2.1 Source

Departmental data
Human Resource
Finance
Procurement

4.2.2 Required inputs/Resources

- Servers, Desk tops and Laptops
- External Hard drives
- WIFI/ Local Area Network facility
- ICT Officers
- Safe air conditioned, dust free room
- Conducive working environment
- Budgetary Allocations

4.2.3 Expected outputs

- Real time Data Backups

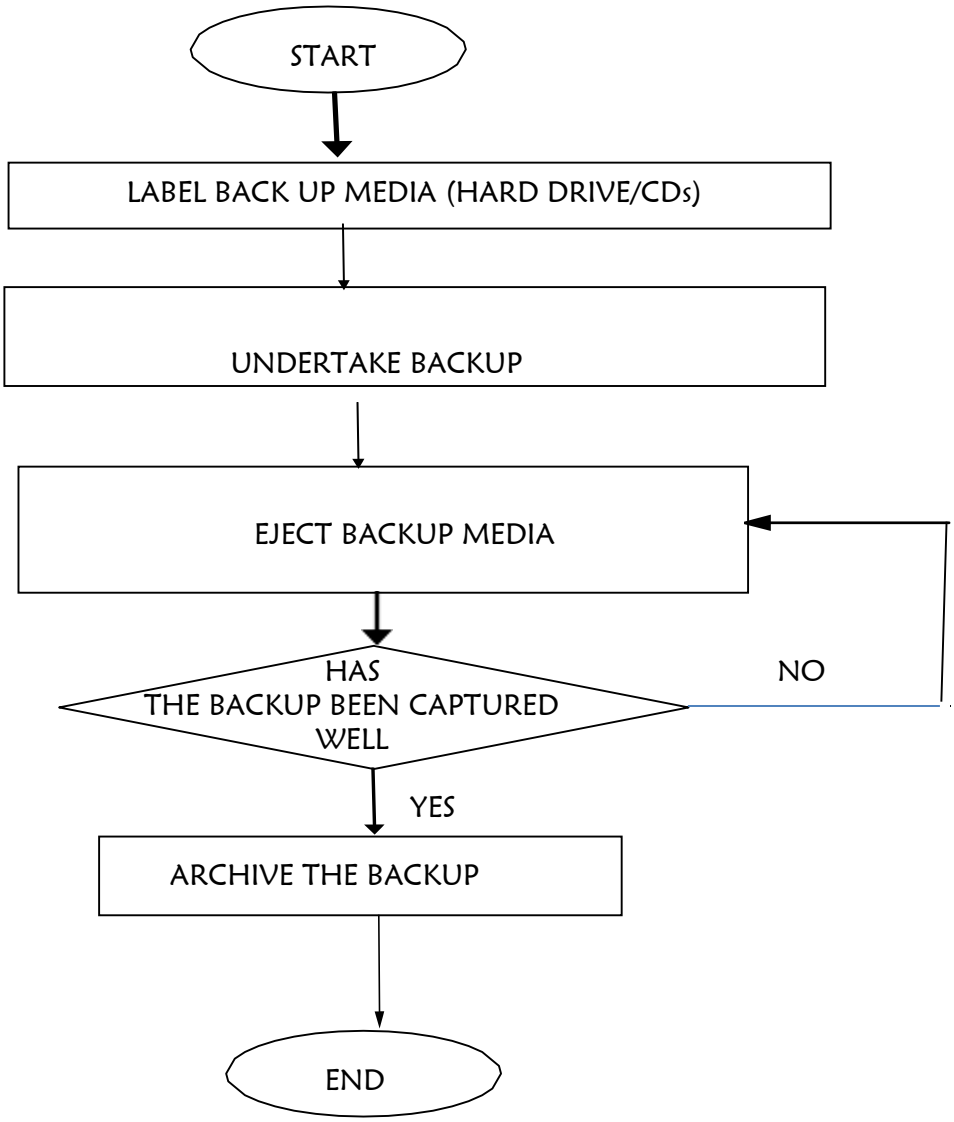
4.2.4 Customers

Management/Users

4.2.5 Procedure details

o.	Process Details/Description	Resources	Responsibility	Timelines	Output	Measure of Success (KPI)
	Label the backup media (hard drive or CDs)	Hard drives CDs	Chief ICT Officer	1 day	Labelled Hard drives/CDs	List of labelled drives/CDs
	Undertake periodic data backup	Server Software Hard drives ICT Officer	Chief ICT Officer	Daily Monthly	Daily Data backups Monthly back ups	Backup drives

		WIFI connectivity				
	Archive the backups safely	Electronic media, hard drives, CDs	Chief ICT Officer	Daily Monthly	Archived back up data	List of archived backups



4.3. Processes for Database recovery NWHSA/FCP/SOP/04/DR

4.3.1 Source

Procurement
Departmental data
Finance
Staff

4.3.2 Required inputs/ Resources

- Servers, Desk tops and Laptops
- External Hard drives
- WIFI/ Local Area Network facility
- ICT Officers
- Safe air conditioned, dust free room
- Conducive working environment
- Budgetary Allocations

4.3.3 Expected outputs

- Data base recovery

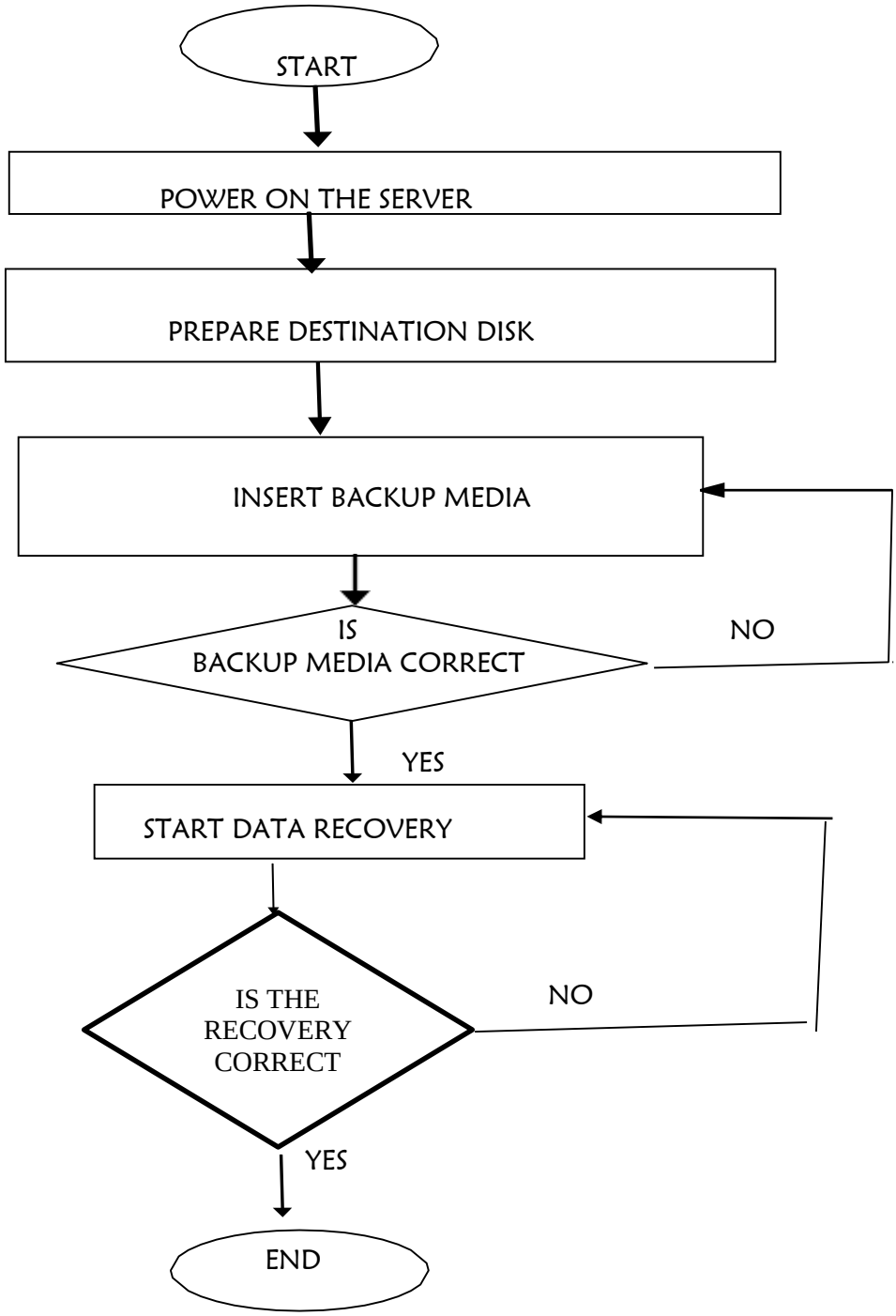
4.3.4 Customers

Management/ Users

4.3.5 Procedure details

No.	Process Details/Description	Resources	Responsibility	Timelines	Output	Measure of Success (KPI)
1.	Power on the Server	ICT Staff Server Secure Server room	Chief ICT Officer	1 day	Powered Server	
2.	Prepare destination Disk	ICT Staff Server	Chief ICT Officer	1 day	Secure Disk	
3.	Insert backup media	Server Hard drive/CD ICT Officer	Chief ICT Officer	1 day	Backup media inserted into the server	
4.	Start data recovery	Server Backup media ICT Officer	Chief ICT Officer	1 day	Data restored	
5.	Verify the correctness	Server	Chief ICT Officer	1 day	Data verified	

	of the data	ICT Officer				



4.4. Process for ICT Equipment Maintenance **NWHSA/FCP/SOP/04/EM**

4.4.1 Source
Human Resource
Finance
Procurement

4.4.2 Required inputs/resources

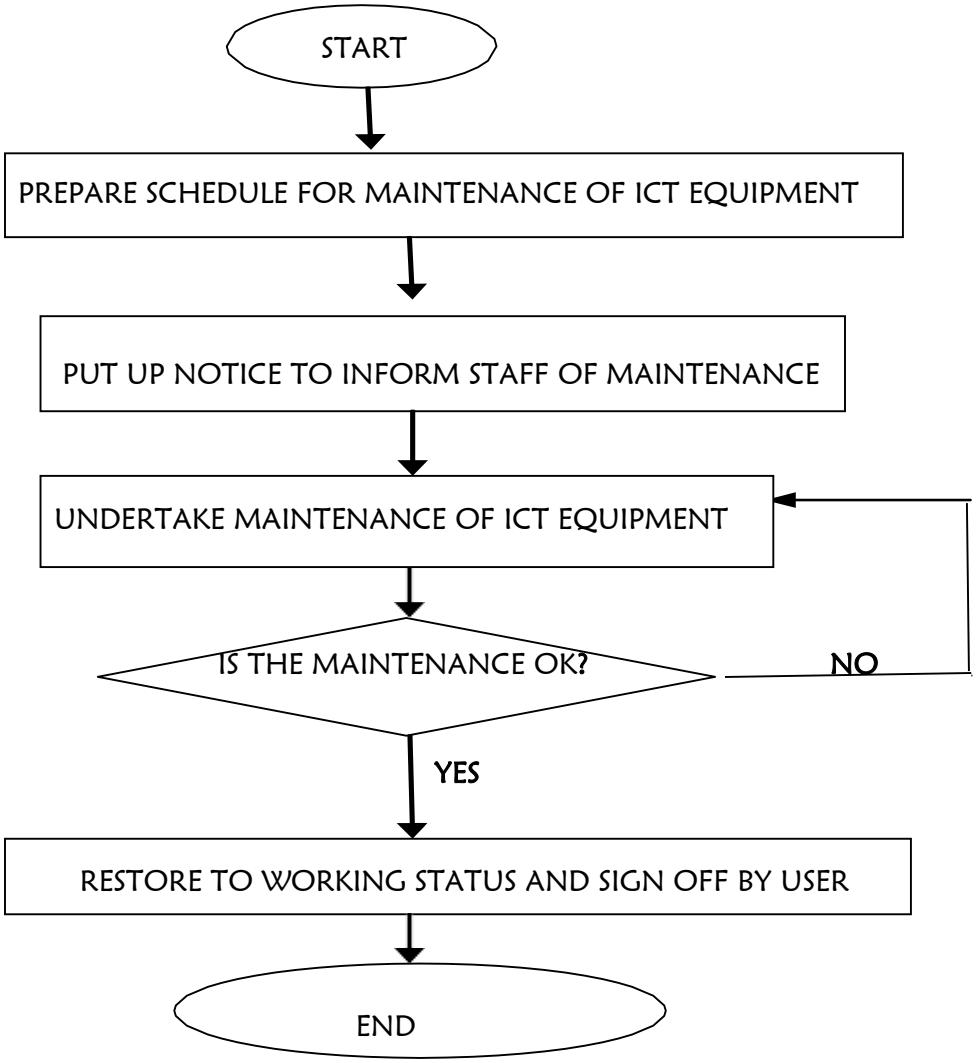
- ICT equipment to be maintained
- ICT Technical staff
- Allocated budget
- Repair and Maintenance toolkit (hardware and software)

4.5.2 Expected outputs

- Quarterly maintenance report

4.4.2 Customers
Employees;

No.	Process Details/Description	Resources	Responsibility	Timelines	Output	Measure of Success (KPI)
1.	Prepare a schedule for servicing of equipment	ICT Staff	Chief ICT Officer	Quarterly	Annual schedule	
2.	Put a notice for staff to take note of the scheduled servicing	Printer Notice board	Chief ICT Officer	Quarterly	Staff informed	Notice on notice board
3.	Undertake the maintenance as per schedule	ICT Technical staff Service Provider Servicing room Users	Chief ICT Officer	1 week	Serviced equipment	Signed work logs
4.	Prepare a maintenance report	Laptop ICT Officer	Chief ICT Officer	1 week	Report	Signed report


START
PREPARE SCHEDULE FOR MAINTENANCE OF ICT EQUIPMENT
PUT UP NOTICE TO INFORM STAFF OF MAINTENANCE
UNDERTAKE MAINTENANCE OF ICT EQUIPMENT
IS THE MAINTENANCE OK?
NO
YES
RESTORE TO WORKING STATUS AND SIGN OFF BY USER
END

5. RECORDS/RETAINED DOCUMENTED INFORMATION

(i) Daily backup logs
(ii) Backup inventory file
(iii) Repairs Report file
(iv) Maintenance file
(v) User accounts file

6. RISK AND MITIGATION MEASURES

RISK	MITIGATION
Data storage media failure	Data backup
Theft and vandalism	-Data -CCTV -Employ Security -Restrict access of computer rooms to only authorized users
Unauthorized access	-Implement authentication and role-based access control -Install intrusion detection systems
Systems network failure	- Help desk Power backup
Bad weather	- Secure ICT area - Weather proof all ICT equipment
Virus attack	- Install antivirus software - Install firewall - Scan gadgets for viruses before inserting in computersr4estrict insertion of external/ removable gadgets
Hacking	- Increase security layers for both software and hardware - Use of modern technology
Obsolete software/ hardware	- Updating systems with the current technology - Have systems/ machine replacement plans
Hardware maintenance not undertaken	- Frequent maintenance of machines
Failure to backup	- Take frequent backups - Have an offsite backup
Insufficient Technical staff	- Recruitment of additional technical staff - Train available staff
Software piracy	- Purchase genuine software