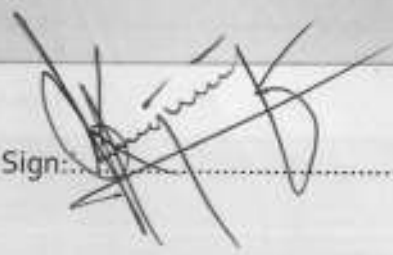
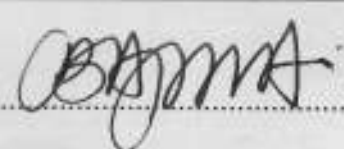
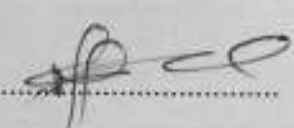



DEPARTMENT	IT & SYSTEMS
TITLE OF DOCUMENT	IT & SYSTEMS DISASTER RECOVERY PLAN
Author / Prepared by:	HEAD, IT & SYSTEMS DEPARTMENT
Date & Signature of Author	Date: 19/10/2023 Sign: 
APPROVED BY:	
Managing Director & CEO	Date: 19/10/2023 Sign: 
Chairman Risk Committee	Date: 19/10/2023 Sign: 
Board Chairman	Date: 19/10/2023 Sign: 

IT & SYSTEMS DEPARTMENT				FCMB PENSIONS LIMITED RC No: 620900	
Date of Last Approval:	28/04/2019	Date Policy Will take effect:	Immediate		
Title of Manual	IT & Systems Department Disaster Recovery Plan				
Author:	FCMB Pensions Ltd				
Custodian / Title & email	Head, IT & Systems Department lukmanyusuf@fcmbpensions.com				
References & Legislation:	<ul style="list-style-type: none"> • Pension Reform Act, 2014 				
Supporting Documents, procedures & other materials:	<ul style="list-style-type: none"> • PenCom Regulation on IT Management • Information Technology Infrastructure Library (ITIL) Standard 				
Audience:	FCMB Pensions staff / FCMB Group				
Next Review Date:	2025				

TABLE OF CONTENTS	
Introduction	iii
Abbreviations	v
Backup & Recovery	Chapter 1 Page 2
Disaster Recovery Plan	Chapter 2 Page 4
Hardware & Software Inventory	Chapter 3 Page 7
Approval Page	Page Ai

Introduction

The IT & Systems Department is responsible for ensuring that all transaction data is recoverable in the event of accidental loss or damage. Disasters may occur at any time for many reasons. Disaster recovery plans are put in place to prevent or reduce the effects of such disasters.

This document shall be known and recognized as the **IT & Systems Department Disaster Recovery Plan**. The fundamental essence of this document is to define the procedure to follow in the event of disaster in line with the **PenCom Regulation** and in tandem and consonance with the extant provisions of the **Pension Reform Act, 2014**.

This step-by-step description of the process and procedure is considered as the minimum applicable standard to ensure effective recovery in the event of disaster at FCMB Pensions Limited and have been put in place for the purpose of clarity of function and simplicity of usage.

The manual has categorized and catalogued the process and procedure for ensuring effective business continuity into the:

- Backup and Restore
- Disaster Recovery Plan

Purpose of the Plan Manual

1. To provide the minimum acceptable rules and standards for disaster recovery in the event of a disastrous event.
2. To ensure that timelines are provided for restoring business operations.
3. To ensure that the individuals responsible for prompt action in the event of disaster are adequately identified.
4. To ensure that the knowledge of processes and procedures is officially documented and available to all stakeholders for reference and for the smooth and seamless execution of duties.

The **IT & Systems Disaster Recovery Plan** has complied with all relevant guidelines and rules issued by PenCom for the IT and Systems Department.

ABBREVIATIONS:

DR	- Disaster Recovery
LAN	- Local Area Network
RTO	- Recovery Time Objective
PenCom	- National Pension Commission
RT	- Recovery Team

IT & SYSTEMS DEPARTMENT

DISASTER RECOVERY PLAN & BACKUP

	DISASTER RECOVERY PLAN	
IT & Systems	Backup & Recovery	Code: FPL_IT_DR_01
	PROCESS DESCRIPTION	

Objective:

To provide guidelines on strategy, plans, and procedures for FCMB Pensions to prevent the loss of information and to implement backup and recovery procedures in order to ensure the confidentiality, integrity, and availability of the electronically protected data and information of the company.

Key guidelines:

- To define strategy, plans, and procedures for ensuring the recoverability of data and information in the event of accidental loss or damage.
- IT & Systems Department is responsible for ensuring that all data is recoverable from backups in the event of accidental loss or damage.
- Ensuring that periodic, scheduled rotation of backup media is being followed for the off-site storage facilities
- If a User creates an important file from their personal workstation, he/she would store that file on the central storage Server so that it will be backed up.
- All media belonging to the organization is assumed to contain sensitive information and should be treated as such.
- Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.

Tape Backup and Restoration

Tape backup should be run weekly on Friday through a pre-schedule or manually started process. This should however be run when none of the file/folder is not in operational state. Once completed, any of the weekly tape must be used for monthly restoration simulation. This can be done by restoring a single folder/file to demonstrate actual restoration before sending the batch to Lagos.

No.	Activities	Description	Responsibility	Support
1.	VEEAM Backup	<ol style="list-style-type: none"> 1. Manage the VEEAM Backup Server at Gwarinpa 2. Check the backup has been successful. 3. Manage a backup failure. 4. Manage VEEAM availability 	Backup Officer	Networker
2.	SAN to SAN Replication on Hitachi SAN	<ol style="list-style-type: none"> 1. Manage SAN to SAN replication from HQ to DR site 2. Check the replication status 3. Manage network bandwidth availability 	Backup Officer	Hitachi SAN
3.	Verification of Backup Status	A check on the backup status on the system and report any failures to the Head, IT & Systems Department. If the backup fails repeatedly, it will be necessary to perform a manual backup. This takes time, and must be performed when all Users have logged out.	Backup Officer	<ol style="list-style-type: none"> 1. Networker 2. Hitachi SAN
4.	Investigation/Resolution	A thorough troubleshooting and fixing of the cause of failure.	System/ Database Administrator.	
5.	Tape Backup	Tape backup is performed on files, folders and databases weekly on Fridays and couriered to Lagos Office	Backup Officer	Tape Drive
6.	Tape Backup Log	A Weekly tape backup log is physically kept to report backups, restores and their status. Any actions taken as a result must be recorded. These logs are stored in a log book located in the IT & Systems Department.	Backup Officer	Logbook
7.	House-keeping of the Backup System	Regular maintenance of the backup server and other storage devices is carried out to ensure it is kept in good working condition.	Backup Officer	
8.	Backup Cycle /Frequency	All data are backed up to a remote location through VEEAM Application on a daily basis	Backup Officer	Networker
9.	Tape Backup Retention	Tape backups are usually retained for a minimum period of three (3) months and reused for another backup once it arrives from Lagos Office.	Backup Officer	Tape

Responsibilities-

Backup Officer – Is responsible for taking the backup, log, and the frequencies as required and verifying the integrity and status of a backup taken and also the best cycle to be restored in the case of a disaster according to stipulated procedures and guidelines in line with best practice.

System Administrator- investigates, maintain, and fix backup equipment and backup devices that failed backup processes.

	DISASTER RECOVERY PLAN	
IT & Systems	Disaster Recovery	Code: FPL_IT_DR_02
	PROCESS DESCRIPTION	

Objective

The primary objective of this Disaster Recovery Plan is to help ensure business continuity by providing the ability to successfully recover Technology Solutions in the event of a disaster.

Specific goals of this plan relative to an emergency include:

- Detailing a general course of action to follow in the event of a disaster.
- Minimizing confusion, errors, and expense.
- Implementing a quick and complete recovery of services.

The secondary objectives of this Plan are:

- Reducing risks of loss of services.
- Providing ongoing protection of institutional assets.
- Ensuring the continued viability of this plan.

Key guidelines:

- The purpose of this policy is to define strategy, plans and procedures for ensuring continuity of FCMB Pensions’ business in the event of any eventuality.
- This plan will provide policies, procedures, roles, and responsibilities for preparing for, responding to, and recovering from a variety of disasters.
- IT & Systems Department is responsible for ensuring that all transactional data is recoverable in the event of accidental loss or damage.

ASSUMPTIONS

This disaster recovery plan is based on the following assumptions:

- The safety of staff is of paramount; the safeguard of such will supersede concerns specific to hardware, software, and other recovery needs.
- Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in this IT Disaster Recovery Plan will be made available.

- Depending on the severity of the disaster, other departments/divisions may be required to modify their operations to accommodate changes in system performance, computer availability and physical location until a full recovery has been completed.
- Management will encourage other departments to have contingency or business continuity plans for their operations, which include operating without IT systems for an extended period of time.

There are many types of disaster that can affect the operations of FCMB Pensions Ltd. with a business site situated at Plot 207, Zakaria Maimalari Street, CBD, Abuja II Abuja and a disaster recovery site situated at **plot 518, Wing B, 4th Avenue, Said Zungur Street Gwarinpa**, Abuja. We could rate the different threats as follows:

Recovery Time Objective RTO

The maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels is 24hrs

SN	Natural Threat	Severity	Recovery Time	Location
a	Fire	High	48 Hours	Gwarinpa
b	Earthquake	Low	48 Hours	Gwarinpa
c	Volcanic Eruptions	Low	48 Hours	Gwarinpa
d	Lightning and Thunderstorm	High	48 Hours	Gwarinpa
e	Windstorm, Tornadoes and Hurricane	Medium	48 Hours	Gwarinpa
f	Snow and Ice Storm	Low	48 Hours	Gwarinpa

Roles and Responsibility of individuals vital for fulfilling business continuity

FCMB Pensions has the following as its emergency response, business continuity and recovery team.

1. ED, Business Development & Operations (**Osarhieme Osaghae - 08033025393**)
2. Chief Financial Officer (Lawrence Keshiro - 0808180004721)
3. Head Operations (Olusegun Ogunsanya - 08039796003)
4. Head Corporate Resources (**Victor Odumodu - 08033385377**)
5. Head IT & Systems (Lukman Yusuf - 08037817002)

The primary responsibilities of the Team include:

1. Activating a portion of the plan
2. Logging the recovery events
3. Ensuring low downtime and prompt business continuity
4. Communication of event status.

Responsibilities of Team Members

No.	Activities	Description	Responsibility	Support
1.	Coordination of recovery activities	Overall coordination and management of recovery activities	Team leader	Team members
2.	Documentation of recovery activities	Adequate documentation of all activities involved in the recovery process.	Head, IT	Team members
3.	Senior management liaison	Communicate with the senior management on the decision of the team.	Team leader	Team members
4.	Plan Execution	Leads the execution of the recovery exercise.	Team leader	HODs
5.	Staff assignments	Assigned staff to various roles during recovery exercise.	Team leader	HODs
6.	Activation of recovery team	Call the recovery team to action whenever the need arise.	Team leader	HODs
7.	Communication with system Users	Communicate with the system users on the status of IT infrastructure required for business continuity.	Head, IT	HODs
8.	Vendor interface	Communicate with various vendors for further support to keep the business up.	Head, IT and Head, CR	Financial Control
9.	Equipment salvage	Take inventory of company's equipment after the recovery exercise.	Head, CR and Head, IT	Team members
10.	Equipment installation	Install company's equipment required to keep the business running.	Head, IT and Head, CR	Team members
11.	Restoration of primary site	Ensure the primary site is back to its normal state prior to the incident.	Head, IT and Head, CR	Team members
12.	Obtain system and other documentations	Provide IT system and other company asset after the incident.	Head, IT and Head, CR	Team members
13.	Prepare recovery site and command center for operation	Ensure the recovery site is up and running to support continuous business operations.	Head, IT and Head, CR	Team members
14.	Establish telecommunication network	Ensure adequate telecommunication is put in place to ensure smooth running of the recovery site.	Head, IT and Head, CR	Team members
15.	Coordinate transportation of people and supplies	Coordinate movement of people and supplies to and fro the recovery site.	Head, CR	Team members
16.	Workload scheduling	Schedule work activity appropriately among the staff.	HODs	Team members

Please Note:

Depending on the severity of the incidence/disaster, other departments/divisions

	DISASTER RECOVERY PLAN	
IT & Systems	Hardware & Software Inventory	Code: FPL_IT_DR_03
	<u>DR INVENTORY</u>	

The following are hardware and software currently at the DR Site

S/No	Names	Type	Total
1	HP Servers	Hardware /Server	3
2	HP Desktop Computers	Hardware /Workstations	20 Sets
3	EMC Data Domain	Hardware	1
4	HP Tape Reader	Hardware	1
5	VEEAM Backup solution	Software	
6	Ms Exchange	Software	
7	Moneytor/IBS	Software	
8	Ms Dynamics 365	Software	
9	Docuware	Software	
10	Sage (Evolution and HR)	Software	
11	Hitachi SAN storage	Hardware	1

APPENDIX

VEEAM BACKUP FREQUENCY

SN	Server	Source Folder on Server	Destination Folder on External Backup System (Networker)	Remark	Frequency	
1	FP-Docuware	E:\Docuware	Docuware	Docuware	Daily	Monthly
2	FP-Exchange	E:\Exchange Backup	Exchange	MS Exchange	Daily	Monthly
3	FP-Sage	E:\SAGE_DUMP\EVOLUTION_BKUP	SAGE Evolution	SAGE Evolution Accounting Package	Daily	Monthly
4		E:\SAGE_DUMP\PAYROLL_BKUP	SAGE Payroll	SAGE Payroll	Daily	Monthly
5	FP-PensionAppDB FP-PensionApp	E:\ScheduledDaily BackUp	Daily Backup	Microsoft Dynamics BC	Daily	Monthly
6	FP-Files	E:\File Server	FileServer	Files used stored by Departments	Daily & Weekly	Monthly
7	FP-IBS-APP FP-IBS-DB	E:\ScheduledDaily BackUp	Daily Backup	IBS	Daily	Monthly

HITACHI SAN STORAGE REPLICATION

SN	Server	Source Folder on Server	Destination Folder on SAN Storage	Remark	Frequency
1	FP-Docuware	E:\Docuware	Docuware	Docuware	Daily
2	FP-Exchange	E:\Exchange Backup	Exchange	MS Exchange	Daily
3	FP-Sage	E:\SAGE_DUMP\EVOLUTION_BKUP	SAGE Evolution	SAGE Evolution Accounting Package	Daily

4		E:\SAGE_DUMP\ PAYROLL_BKUP	SAGE Payroll	SAGE Payroll	Daily
5	FP- PensionAppDB FP-PensionApp	E:\ScheduledDailyBack Up	Daily Backup	Microsoft Dynamics BC	Daily Backup
	FP-IBS-APP FP-IBS-DB	E:\ScheduledDailyBack Up	Daily Backup	IBS	Daily Backup
6	FP-Files	E:\File Server	FileServer	Files used stored by Departments	Daily & Weekly


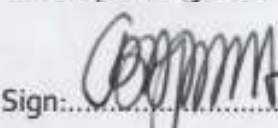


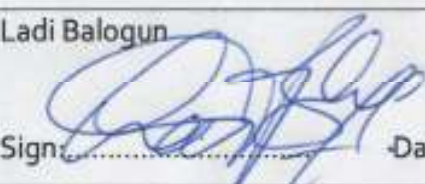
TAPE BACKUP FREQUENCY

SN	Items	Source Folder on Server	Destination Folder on External Tape	Remark	Frequency
1	FP-Sage	D:\LPML\EVOLUTION COMMON_BKUP	/SageEvolution	SAGE Evolution Accounting Package	Weekly
		E:\SAGE_DUMP\ 	/SAGE Payroll	SAGE Payroll	Weekly
2	FP- PensionAppDB FP-PensionApp	G:\DYNAMICS BC BackUp G:\HrWorkplace Backup	/Navision	Microsoft Dynamics BC	Weekly
3	FP-Files	E:\File Server	/FileServer	Files used by all Departments	Weekly
4	FP-IBS-APP FP-IBS-DB	H:\ScheduledDailyBack Up	/IBS	IBS	Weekly

DATA RETENTION

Tape Backup Retention	Tape backup must be retained for a minimum period of three (3) months and reused for another
Backup to SAN	Backup to SAN must be retained for a minimum of one year before it can be overwritten.

APPROVAL PAGE

IT & SYSTEMS DEPARTMENT	
Designation	
Head, IT & Systems Department	<p>Lukman Yusuf</p> <p>Sign:  Date: 21/07/19</p>
Executive Director, Operations & Services	<p>Christopher Bajowa</p> <p>Sign:  Date: 18/4/19</p>
Managing Director/CEO	<p>Misbahu Yola</p> <p>Sign:  Date: 18/07/19</p>
Chairman, Board Risk Management Committee	<p>Suzanne Iroche</p> <p>Sign:  Date: 30/7/19</p>
Chairman, Board of Directors	<p>Ladi Balogun</p> <p>Sign:  Date: 30/7/19</p>