
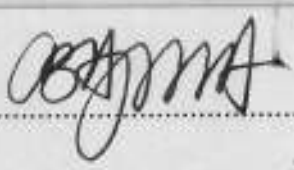


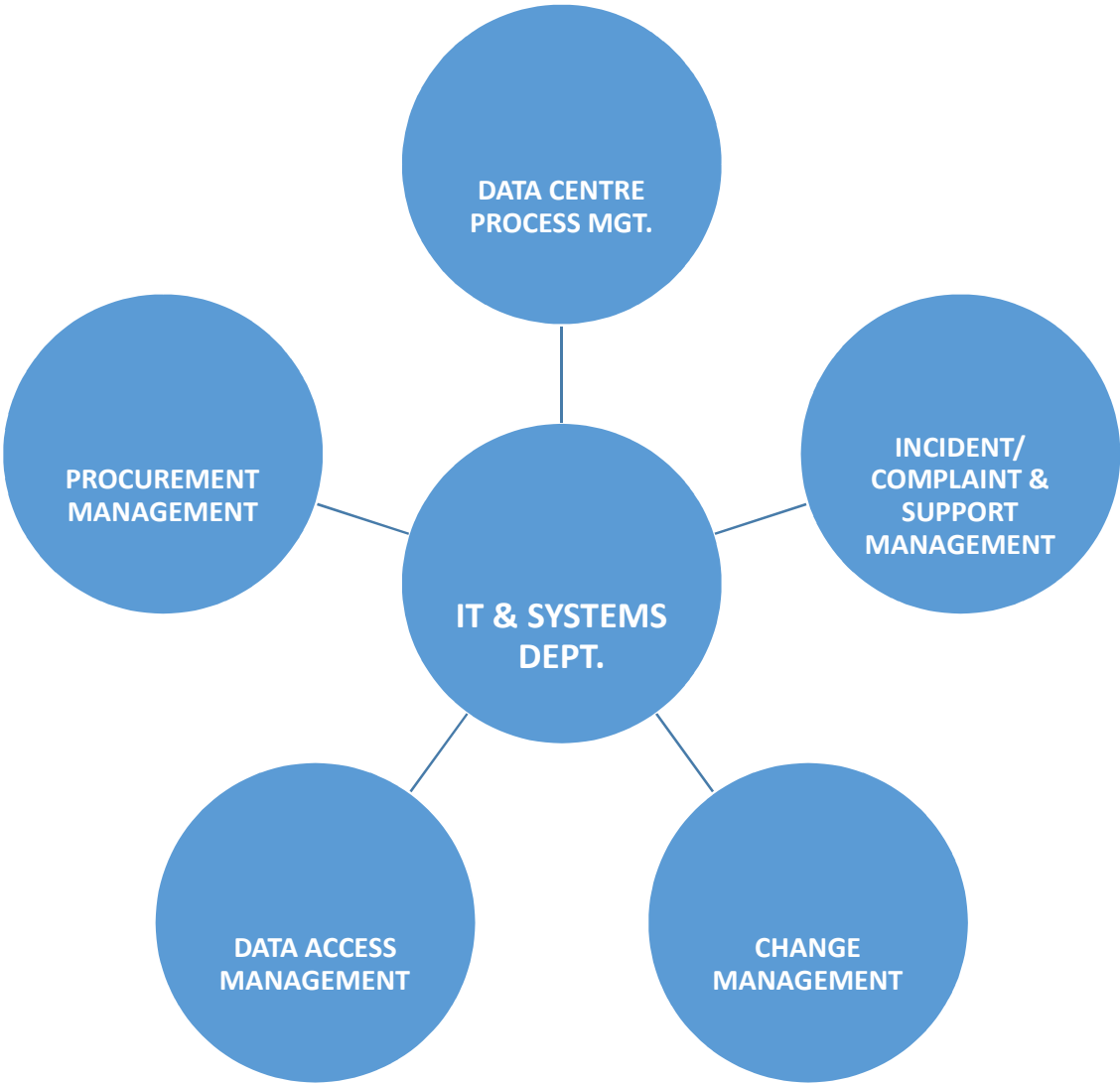




DEPARTMENT	IT & SYSTEMS
TITLE OF DOCUMENT	IT & SYSTEMS STANDARDS OPERATING PROCEDURE
Author / Prepared by:	HEAD, IT & SYSTEMS DEPARTMENT
Date & Signature of Author	Date: 19/10/2023 Sign: 
APPROVED BY:	
Managing Director & CEO	Date: 19/10/2023 Sign: 
Chairman Risk Committee	Date: 19/10/2023 Sign: 
Board 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 Standards Operating Procedures				
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				

**FCMB Pensions Limited
IT Standards & Procedures**



CONTENTS

1. DEFINITIONS.....	3
2. MORNING TASKS/EVENTS.....	4
<i>Application Check</i>	4
<i>Check the Status of Schedule SMS and E-mail Propagation</i>	5
3. DATA CENTER PROCESS MANAGEMENT.....	5
<i>Introduction</i>	5
<i>Power</i>	6
<i>Cooling</i>	8
<i>Servers and Storage</i>	8
<i>DATA CENTRE FLOW</i>	11
4. PROCUREMENT PROCESS MANAGEMENT	12
4.1 <i>Software Acquisition Procedure</i>	12
4.2 <i>Hardware and Peripheral (Consumables) Procurement</i>	13
5.0 CYBERSECURITY AND GENERAL INCIDENCE & HELPDESK MANAGEMENT PROCESS	14
6. REGISTRATION/DE-REGISTRATION OF DATABASE.....	19
7. SOFTWARE INSTALLATION PROCEDURE	19
8. USER ACCESS MANAGEMENT (CREATION AND REVOCATION) PROCEDURE	19
9. USER ACCESS RIGHT ON APPLICATION (GRANT/REVOKE ACCESS).....	24
10. IT CHANGE MANAGEMENT.....	25
10.4 <i>THE CHANGE CLASSIFICATION</i>	26
10.5 <i>CHANGE MANAGEMENT PROCESS</i>	27
11. TAPE BACKUP PROCEDURE.....	31
12. EVENING/CLOSING TASK.....	33
<i>IT Request Form</i>	38
<i>IT Change Request Form</i>	39
13. WORKSTATION MANAGEMENT PROCEDURE	34

1. DEFINITIONS

- **ITSC** – Acronym for IT Steering Committee.
- **SQL Services**-Acronym for Structured Query Language Services.
- **ASP.NET Services**–Active Server Page Services.
- **UPS**–Uninterrupted Power Supply
- **PHCN** – Acronym for Power Holding Company of Nigeria
- **DNS** – Acronym for Domain Name Services.
- **IIS Services**-Acronym for Internet Information System Services.
- **SAN**–Storage Area Network.
- **RPC**–Remote Procedure Call
- **IVR** – Acronym for Interactive Voice Response
- **MD**–Managing Director
- **ED**-Acronym for Executive Director
- **CFO**– Acronym for Chief Financial Controller
- **SMS**–Short Messaging System

2. MORNING TASKS/EVENTS

First thing in the morning, the department performs the below routing tasks to ensure smooth operation of the day:

Access the server room using the provided biometric device.

2.1 Application Check

- Login to the servers hosting the different applications using your username and password.
Refer to 3.3 for server IPs.
- Type in services in the search box and click on services. This will launch the Services module.
- Check the status of all 'Services' and ensure that the status shows 'Started'.
Refer to 3.3 for the required services
- Ping all the servers on which the various applications are residing by pressing the windows key and R.
Type in the IP and click on Enter.

If it responds without timing out, it means it is connected. If it fails, check the network cables connected to the servers.

If all network cables are connected properly and it still times out, check the resources such as storage, memory etc. and ensure they are not maxed out.

If connection issues persists, escalate to the Application's team to troubleshoot.

- Check the status of all external links (branch portal, member self-service, company website) by logging into them using your credentials.

Refer to 3.3 for links or log into the intranet and click on the Apps dropdown to gain access to all applications.

- Check the status of the scheduled daily/weekly backups.
 - Log into 172.16.80.38 and 172.16.80.23
 - Go to PC- Backup (H: drive) – Backup – Daily/Weekly folder.
 - Ensure that the backup done for the previous day/week is there.
- Logout of the server and proceed to the day tasks.

2.2 Check the Status of Scheduled SMS and E-mail Propagation

- Log into EnpowerAdmin application using your details.
(<https://web.fcmbpensions.com/EnpowerAdmin/>)
- Click on Menu then click on Contributions SMS Report.
- Choose required date to get a summary of sent SMS.
- Note that Pending and Outstanding columns have to report zero. This shows that all SMS was sent successfully.

For Email

- Remote to 172.16.80.21.
- Click on Link IT, click on Timothy and then on Statements.
- The automated processes are scheduled and are run at different times and varying frequencies. Most of them are executed daily while others are run on demand.

3. DATA CENTER PROCESS MANAGEMENT

Introduction

This section covers the various processes and procedures to ensure that the Data Centre is up and running at optimal performance from power, server, cooling system, fire safety, to security and network system.

3.1 Power

The Data Centre is powered from two power sources; namely PHCN/Generator, which is the primary power source and Inverter – this is the secondary (back up) source which keeps the data center running in the event of a power failure from the primary source.

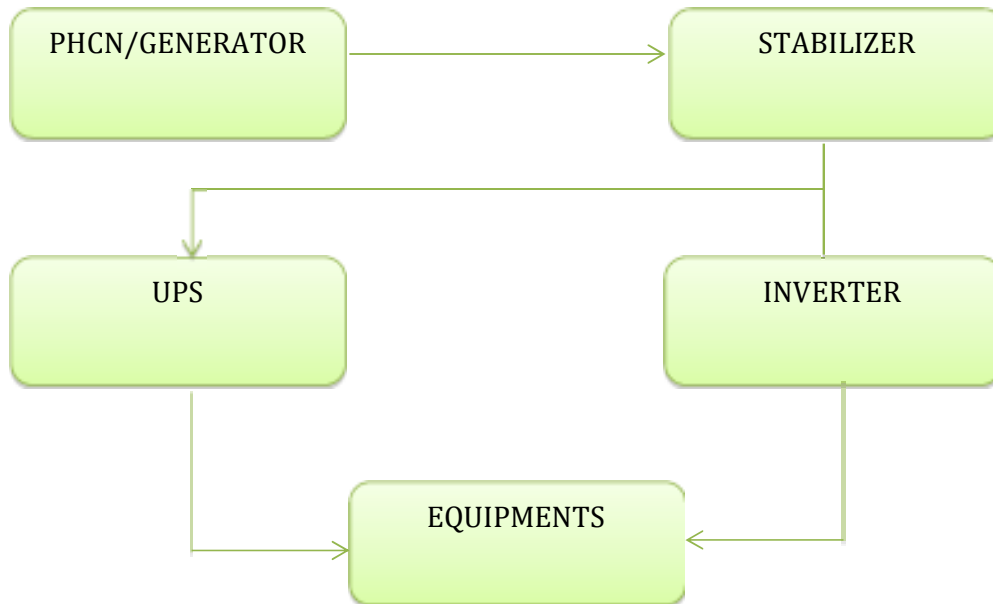
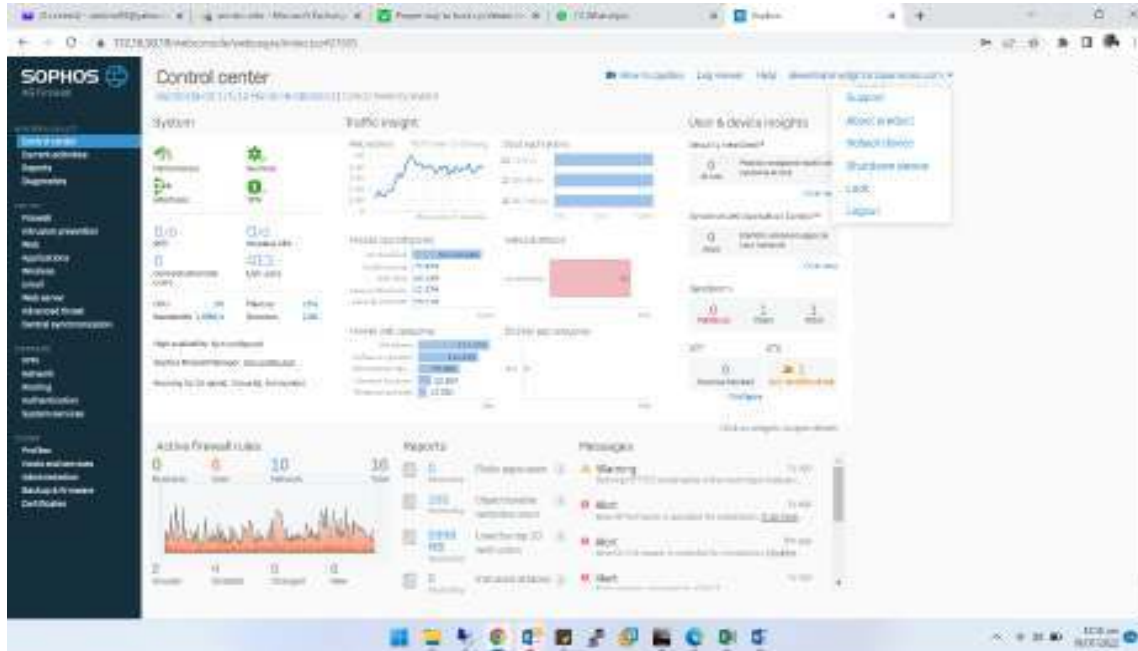


Figure 1. Power Flow

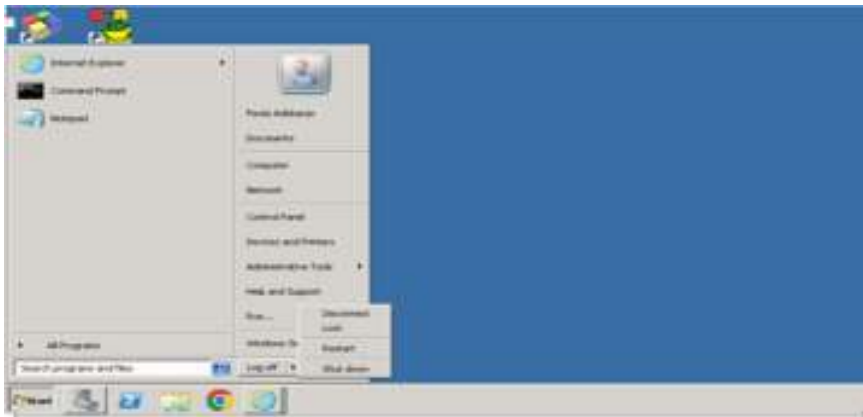
Power from primary source is passed on to the Stabilizer, which in turn supplies power to the UPS. The UPS passes power to the equipment's and the back-up power source (Inverter). The Inverter maintains the power supply in the event of power failure from primary source.

Switching Off Switches, Routers, Servers and Cyberoam.

- Log into the equipment listed above using the connected systems.
- Run the shutdown command for switches and routers.
- Cyberoam has a shutdown module. Simply click on it.



- For servers, Log into the servers using your login details.
- Go to start and select power. Click on shutdown.



Powering Off Stabilizers and UPS.

- Power off the 63A power breaker. This controls the servers and inverters.
- Power off the 200A power breaker. This controls the 100KV stabilizer and the UPS.
- Switch off the stabilizer.
- To power off the UPS. On the Shutdown menu, click Manual Shutdown. The Manual Shutdown dialog box appears.
- Select the UPS component to power-off.
- In the Power-on delay area, select an option to specify when the component is restarted.
- Click Shut Down.

- Click OK to verify the shutdown should begin.
- The shutdown begins.
- Switch off all ACs.

3.2 Cooling

There are 4 cooling units in the data center. All of which are connected to the primary power source, with additional generator dedicated to the data center and first floor. In the event of a complete power failure, all the cooling units will automatically be powered on by the additional generator.

3.3 Servers and Storage

There are two server racks, one for the Storage Server (SAN), and communications equipment, and the other for the Blade Servers (Gen8), Housing eight (8) set of blade servers.

Test Server (172.16.80.107 - 109)

Services:

- SQL Services
- ASP.Net services
- Web Client Services

FP-DOC Server (172.16.80.59)

Services:

- SQL Services
- ASP.Net services
- Web Client Services

Exchange Server (FP-Exchange 172.16.80.41)

Services:

- RPC Local
- Cyberoam Transparent Authentication Suit
- Microsoft Exchange Active Directory Topology
- All Microsoft Exchange Services
- MapiLab POP3 Connector
- DNS Client Services
- Net Logon Services

Web Server (FP-Web-01 172.16.80.37)

Services:

- SQL Services
- ASP.Net services
- Web Client Services

Database Servers (172.16.80.38/50)

Services:

- SQL Services

File servers (172.16.80.48)

Services:

- SQL Services
- Net Logon Services

Sage/Payroll Server (172.16.80.53)

Services:

- SQL Services

Application Server (172.16.80.23/44/57)

Services:

- SQL Services
- IIS Services
- ASP.Net Services
- Remote Access Services

LINKS

Digital onboarding - <https://web.fcmbpensions.com/onlineenrollment>

Branch portal - <https://web.fcmbpensions.com/clientportal/Account/Branch>

BackOffice - <https://web.fcmbpensions.com/onlineenrollment/BackOffice>

Data Recapture- <https://web.fcmbpensions.com/datacapture/logon.aspx>

Enrollment- <https://web.fcmbpensions.com/enrollment/Login.aspx>

PenCom RTS- <https://rts.pencom.gov.ng/rts/faces/login.jsf>

3.4 OTHER SERVERS

IVR Server (172.16.80.24)

In the event of failure of any of the server

- The IT staff first identify the cause(s)
- Rectify it and repower on the server
- Check all the services.
- Log the incident in the Incidence Log Book

3.5 SERVERS AT DR SITE

- Exchange Server (172.16.40.18)
- APPS Server (172.16.40.23)
- File Server (172.16.40.21)

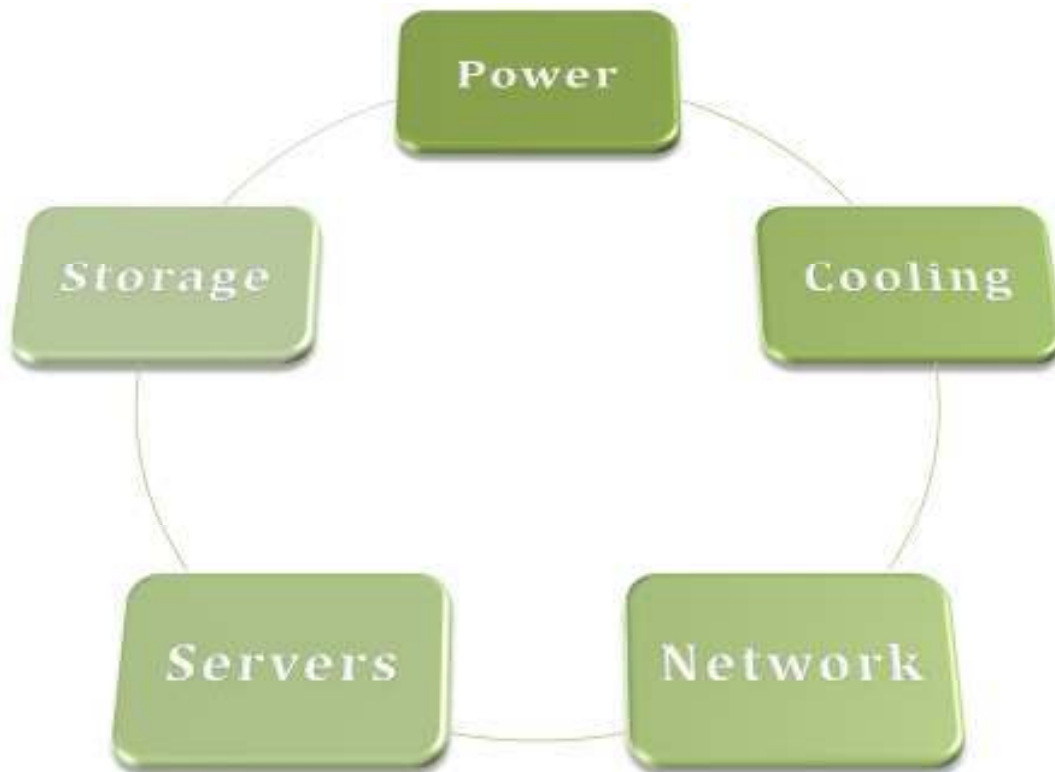
3.6 Network

The whole office is interconnected through a Local Area Network, which is powered by a rack consisting of a Router, Cyberoam Switch, and Cisco Switches.

In the event of outright power failure:

- The IT staff ensures that the core switch is powered on, along with all the other switches and router.
- Ensure that all connections are intact

3.7 DATA CENTRE FLOW



4. PROCUREMENT PROCESS MANAGEMENT

4.1 Software Acquisition Procedure

A feasibility study must be carried out to determine a need for software and, the feasibility study report shall contain documentation that supports a decision to acquire software.

4.1.1 Steps

- A request for proposal (RFP) shall be developed and sent by ITSC to various vendors where the solution is not specific to a single vendor. The (RFP) shall be sent to at least three vendors.
- The ITSC team needs to carefully examine and compare the vendors' responses to the RFP.
- After the RFP have been examined, the project team may be able to identify a single (or two in some cases) vendor who stands out from the rest.
- If more than one vendor is selected, the project team will be advised to talk to one or more current users of each of the potential products.
- An on-site visitation may be considered if it is cost effective
- The discussions with the current users should concentrate on each vendor's:
 - Reliability – Are the vendor's deliverables (enhancements or fixes) dependable?
 - Commitment to Service -- Is the vendor responsive to problems with its product?
 - Does the vendor deliver on time?
 - Commitment to Providing Training and Documentation for its Product
 - What is the level of satisfaction?
- Based on the RFP responses from discussions with current users, the project team can make a product selection. The reason for making a particular choice should be documented.
- The last step in the acquisition process is to negotiate and sign a contract for the chosen product. The contract should contain the following items:
 - Specific description of deliverables and their costs
 - Commitment dates for deliverables and their costs
 - Commitment for delivering of documentation, fixes, upgrades, new release notifications and trainings
 - Allowance for software escrow agreements if the deliverables do not include source code.
 - Description of the support to be provided during installation
 - Provision for reasonable acceptance testing period before the commitment to purchase is made
 - Allowance for changes to be made by the company
 - Maintenance Agreement
 - Allowance for copying software for use in business continuity efforts.

4.2 Hardware and Peripheral (Consumables) Procurement

4.2.1 Steps (User Requests)

- All users requesting for hardware and peripherals shall fill out a request form (See Appendix). The form must be approved by the Head of the Department.
- The form is submitted to IT department for processing.
- The IT department confirms that the user's request is genuine and that there are no alternative means of meeting such request, they shall comment on the request form.
- The IT department will call vendor(s) to bring invoice for the item(s)
- The invoice(s) is scan with the request form and upload to SAGE application for processing.
- The request is route to Account for coding and send back to Head, IT.
- The Head, IT route it back to CFO for his approval (CFO may route it to ED or MD depending on the type and cost of the request).
- Once approved, the request is route back to IT, to print the Purchase order.
- IT department will then ask the approved vendor to bring the item(s)
- Once the item reaches the department, the assigned IT Staff, will sign on the delivery note to confirm that the item(s) correlate to the specification as stated on the Purchase Order.
- The purchase order and the delivery note are passed to Internal Audit/Risk Department for vetting.
- Once vetted, the item is deliver to the requestor
- The requestor will be asked, to fill Equipment Allocation form (in the case of non-consumables).
- The purchase order, request form, invoices and delivery note are passed to Account Department for payment and processing.

4.2.2 Desktop\Workstation Management Procedure.

- The workstation is added to the company's domain. (fcmbpensions.com)
- Workstation naming- Computers will is named following the company's computer naming convention as established by the department.
- The System is configured to enable the assigned staff log in.
- All necessary applications are installed. Such as McAfee Antivirus, AnyDesk, browsers, VPN and printers.
- Deployment of Bit locker for Head Office workstations.
- Access to the necessary Departmental folders is granted to serve as backup for the workstation.
- The staff fills and submits an equipment allocation form after which the workstation is handed over to him/her.

5.0 CYBERSECURITY AND GENERAL INCIDENT & HELPDESK MANAGEMENT PROCESS

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

5.1 Definitions

5.1.1 Customer

The Customer of an IT Service is the staff utilizing the service managed by the IT & Systems Department.

5.1.2. Impact

Impact is determined by how many staff or functions are affected. There are three grades of impact:

- 3 - Low – One or two staff. Service is degraded but still operating within specifications
- 2 - Medium – Multiple staff in one physical location. Service is degraded and still functional but not operating within specifications. It appears the cause of the incident falls across multiple service providers
- 1 - High – All users of a specific service. Staff from more than one department are affected.

The impact of an incident will be used in determining the priority for resolution.

5.1.3. Incident

An incident is an unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Failure of any Item, software or hardware, used in the support of a system that has not yet affected service is also an Incident.

An incident occurs when the operational status of a production item changes from working to failing or about to fail, resulting in a condition in which the item is not functioning as it was designed or implemented. The resolution for an incident involves implementing a repair to restore the item to its original state.

5.1.4. Priority

Priority is determined by utilizing a combination of the incident's impact and severity.

5.1.5. Response

Time elapsed between the time the incident is reported and the time it is assigned to an individual for resolution.

5.1.6. Resolution

Service is restored to a point where the customer can perform their job. In some cases, this may only be a work around solution until the root cause of the incident is identified and corrected.

5.1.7. Severity

Severity is determined by how much the user is restricted from performing their work. There are three grades of severity:

- 3 - Low - Issue prevents the user from performing a portion of their duties.
- 2 - Medium - Issue prevents the user from performing critical time sensitive functions
- 1 - High - Service or major portion of a service is unavailable

The severity of an incident will be used in determining the priority for resolution.

5.1.8. Incident Scope

The Incident process applies to all specific incidents in support of larger services already provided by the IT & systems Department.

5.1.9. Exclusions

- Request fulfilment, i.e., Service Requests are not handled by this process.
- The need for restoration of normal service supersedes the need to find the root cause of the incident.
- The process is considered complete once normal service is restored.

5.2. Inputs and Outputs

Input	From
Incident (verbal or written)	Customer
Output	To
Standard notification to the customer when incidence/complaint is resolved.	Customer.

5.2.1 Roles and Responsibilities

- End user's responsibility: Users are to note their error message as display on the system/application
 - Identify the application (Dynamics 365, Moneytor, Docuware, LegendCRM, Ms Office etc) you are working with when the issue happened.
 - What were you actually doing when it happened? (Opening, printing, sharing etc)
 - Please provide the following details when calling IT: Name, department/branch, equipment name, problem description and other details that might help us resolve your issue.
- IT Staff Responsibilities may be delegated, but escalation does not remove responsibility from the individual accountable for a specific action in the department.

5.3. Incident Categorization, Target Times, Prioritization, and Escalation

5.3.1. Categorization

The goals of proper categorization are:

- Identify Service impacted and escalation timelines
- Indicate which IT staff needs to be involved
- Provide meaningful metrics on system reliability

5.3.2. Priority Determination

The priority given to an incident that will determine how quickly it is scheduled for resolution will be set depending upon a combination of the incident severity and impact.

Incident Priority			Severity		
			3 – Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions	1 - High Service or major portion of a service is unavailable
Impact	3 – Low - One or two staff - Degraded Service Levels but still processing within SLA constraints	3 – Low	3 - Low	2 - Medium	
	2 – Medium - Multiple staff - Degraded Service Levels but not processing within SLA constraints - It appears cause of incident falls across multiple functional areas	2 - Medium	2 - Medium	1 - High	
	1 – High - All users of a specific service - Staff from multiple agencies are affected	1 – High	1 - High	1 - High	

5.3.3. Target Times/ Time lines

Incident support for existing services is provided between 8am and 5pm and may be extend beyond as the case required. 5 days per week throughout the year. Following are the current targets for response and resolution for incidents based upon priority.

Priority	Target	
	Response	Resolve
3 - Low	90% - 9 hours	90% - 5 days
2 - Medium	90% - 2 hours	90% - 4 hours
1 - High	95% - 15 minutes	90% - 2 hours

5.4 Incident/Complaint & Support Management Summary

5.4.1 IT Support Operations are expected to:

- Own all reported incidents/complaints
- Ensure that all incidents/complaints received by the unit are filed
- Identify nature of incidents based upon reported issues and categorization rules
- Prioritize incidents based upon impact to the users and guidelines
- Correct the issue or provide a work around to the customer that will provide functionality that approximates normal service as closely as possible.
- Responsible for incident/complaint closure
- Performs post-resolution customer review to ensure that all work services are functioning properly and all incident documentation is complete
- Notify system administrator of Incidents resolved/unresolved

5.4.2 IT Helpdesk Process Flow

Time of Operation: Monday – Friday 8:00am – 5:00pm

Saturday & Sunday: 10:00am – 4:00pm (Upon Approval)

- All support problems are to be directed to the help Desk:
 - 2024 and 2025 (Head office only)
 - 09038853016 (Branch Offices)
 - Email: it&systems@fcmbspensions.com
- Staff can call/send email to the department to lodge complains. IT staff will if possible, resolve the issue directly on the phone or through email.
- Any issue that cannot be resolved via phone/email will be physically checked (if within the head office), and escalated if possible (for branch offices).
- In case the issue(s) cannot be resolve even after physical check, such issue will be escalated to superior staff for prompt resolution.

- The complainant may be asked to fill IT Complaint form' (See Appendix) for the department to document the incidence. The issue will be categorized and prioritize upon receiving the form.

5.4.3 Supported Systems and Applications

Listed below are the systems and applications supported by the IT & Systems department. The list will be updated as the need arise.

- Windows Operating Systems (7, 8, 10)
- MS Office (2007, 2013, 2016)
- Dynamics 365
- Moneytor IBS
- Docuware
- LegendCRM
- Reeltech
- Qlikview
- McAfee and Windows Defender Anti-virus
- Web Browsers (Chrome, Edge, Internet Explorer, Firefox)
- Adobe acrobat reader
- Sage (Evolution and Pastel)
- Bloomberg
- Enrolment System
- Official Laptops
- Official Desktop computers
- Official Printers and Scanners
- CISCO IP Phones
- Projectors
- CCTV
- Access Control Cards
- ManageEngine

5.4.4 Un-Supported Systems and Applications

The department will provide their best knowledge for unsupported systems and applications. However, this is not guaranteed if the product is unfamiliar and little information about it is available. The department will not provide support for cracked software and laptops/computer brought from home.

6. REGISTRATION/DE-REGISTRATION OF DATABASE

Whenever there is need to grant access to or revoke access to database, the process below must be strictly adhered to.

- IT personnel fill the registration/deregistration of database form and submit to the Head, IT & Systems
- Head, IT & System reviewed the request
- Head, IT & System seek approval from the ED OPS
- ED OPS approves/disapproves the request
- Head, IT & System will implement the decision of the ED OPS through the System Administrator.

7. SOFTWARE INSTALLATION PROCEDURE

To install new software on the user's PC, the following procedure must be strictly followed:

- The Head IT & Systems or System administrator or the assigned IT staff will identify the required software and computer
- The assigned IT staff picks the installation media from the Library or load from 'IT shared drive' (in case of non-disc installation)
- The software is installed on the required computer and tested to ensure successful operation
- The installation media is return to the Library for safe keeping.

8. USER ACCESS MANAGEMENT (CREATION AND REVOCATION) PROCEDURE

8.1 Account Management: User accounts are the primary form of digital identity and access to the company's computing resources. As such, it is vitally important that these digital identities be managed in a consistent manner. The following outlines account management practices for the FCMB Pensions Ltd.

Account Format: The following naming standards will be used for all accounts created within the company's computing environment.

- User accounts: first name+last name (e.g. Lagos Nigeria will be lagosnigeria)
- email: firstname+lastname@domain.com (e.g. Lagos Nigeria will be: lagosnigeria@fcmbpensions.com)
- User account must be unique within and across computing platforms including group mail

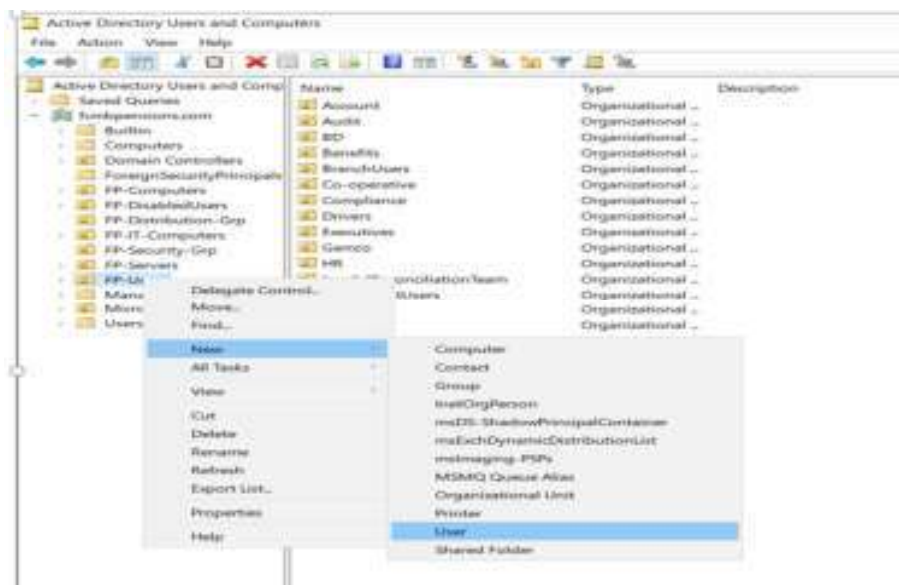
8.2 Account Creation/Access Procedures

A request for a new account should be originated from Corporate Resources (CR) to IT & Systems through either email, or user creation form with the following key details:

- Requester's Name
- Name of the new staff
- Job title of the new staff and other details
- Services required (default services are: MS Outlook, MS Office and Intranet access)

User Creation On Active Directory

- Log into the AD server with your credentials.
- Right click on Start and select Active directories and users.
- Right click on FP-Users and select new and then select user.



- Fill in the staff details as sent by Corporate Resources and then click on ok.

Upon creation, IT & Systems will send the account created details to CR detailing user's credentials. It is the responsibility of CR to communicate same to the respective user.

- If further access to specific application is required, the staff upon successful login to assigned computer should approach IT & Systems department for 'User Access Creation Form'

User Creation on Applications

- Log into EnpowerAdmin (<https://web.fcmbpensions.com/EnpowerAdmin/>)
- Click on menu and select create new user in the description bar.

The screenshot shows the 'ENPOWER ADMIN' dashboard with a 'Dashboard' header. The main content area is titled 'The Agent Code is available' and contains a form for adding a new user. The form fields are arranged in two columns:

- Left Column:** Staff ID (dropdown), First Name, Middle Name, Email, Zone (dropdown), User Name, Password.
- Right Column:** Role (dropdown), Last Name, Gender (dropdown), Mobile, Location/State (dropdown), Branch (dropdown), Confirm Password.

Below the form are three checkboxes: WSA Tagging, Disregard, and Lock Account. A 'Save' button is located at the bottom of the form.

- Type in the Staff ID to verify if the staff has been created.
- Fill in the new user details and save.
- Log into enrollment with your Staff Id (<https://web.fcmbpensions.com/enrollment/Login.aspx>)
- Go to Users and check which app you want to add the user to.
- Go to Roles. Select the app and click on users.
- Type in the User ID.
- Click on Add to List.
- Save.

Addition to Group Mails & Shared Folders

- Log into the AD server
- For addition to group mail, double click on Distribution group, double click on the needed mail group.
- Select member, click add. Type in the name of the staff.
- Click apply and click on ok.
- For addition to shared folder, double click on Security group, double click on the needed shared folder.
- Select member, click add. Type in the name of the staff.
- Click apply and click on ok.

Uploading TW Clients into Back Office from RTS.

- Log into RTS portal using your credentials.
- Input the token and login in.



- Select Transfer request
- Select Detailed RTR Submissions.
- Select date and spool.



- Download spooled excel
- Log into back office
- Select Requests under the transfer window Menu
- Click on Import
- Choose File and import.

- Confirm by checking PINs randomly.

Reset Back office online Password.

- Log into Back office
- Reset Online User Password
- Enter either phone number or Email of client
- Reset Password.

8.3 Managing Privileges

- A user account should have the least privilege that is sufficient for the user to perform their role within the company. Access to information and information systems and services must be driven by business requirements.

8.4 Revoking Access (Deactivation Process)

The following procedures specify the requirements for deactivation of employees account.

Corporate Resources will submit a request for deactivation to the IT & Systems to have an account disabled through email. With the following details:

- Requester's Name
- Name of the staff concerned
- Department and other details
- Reason for deactivation
- Effective date

User accounts shall be disabled immediately once IT received instruction from CR detailing the above. All system logons and access to all network services and applications shall be revoked. Reactivating an account that has been disabled as a result of re-employment or other reason(s) will require the CR to follow the initial account creation request process

8.5 Employees on Suspension

Computer account access of employees who are on suspension will be locked. During the employee's absence, access to the contents of their e-mail, local and network file space may be granted to a co-worker or supervisor at the department HOD's request. The request must come from the HOD through email requesting the transfer of the account access and the designated employee.

8.6 Temporary Privilege Accounts:

Temporary privilege accounts will only be issued at the discretion of the Head, IT & Systems with the approval of Executive Director. Duration of such accounts will be negotiated based upon the business need and only when there is no viable alternative solution. These accounts will be limited in function, allowed only to perform the required task/s or projects: When privileges are granted for a particular project, these privileges will be revoked at the completion of the project.

9. USER ACCESS RIGHT ON APPLICATION (GRANT/REVOKE ACCESS)

Whenever there is request to install software or grant user access to the applications the following procedure must be strictly adhered to.

- The HOD identified staff that requires the software installation or access right.
- The staff proceeds to IT & Systems dept. to obtain 'USER ACCESS CREATION/SOFTWARE INSTALLATION FORM.
- The form is passed to respective HOD to append their signature
- The form is submitted to IT & Systems
- The IT & Systems reviews it and seek approval from the ED OPS
- ED OPS approves/disapproves the request
- The IT & Systems grant/revoke access as approved and notify the personnel concerned through email.
- For revocation due to transfer/termination/resignation/retirement, the steps in **(8.4)** shall be followed.

10. IT CHANGE MANAGEMENT

IT Change Management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management Process begins with the filling of a Change Request form and ends with the approval or disapproval as the case may be.

DEFINITIONS

- **CR** – Change Request.

10.1 Objectives and Principles

The objectives of the IT Change Management Process are to:

- Enforce an evaluation of a proposed change in terms of its benefit, cost, and risk to the systems, and the implications of the change to business activities;
- Ensure users are involved in changes to and development of the application software(s) and hardware deployment;
- Ensure that all changes undertaken are tested against compliance with the National Pension Commission.

10.2 Scope of the Change Management Process

The intended scope of the Change Management Process is to cover all of the company's computing systems and platforms. The primary functional components covered in the Change Management process:

- ❑ Hardware – Procurement, reconfiguration and relocation.
- ❑ Software – Installation, patching, upgrade or removal of software products including operating systems, commercial off-the-shelf (COTS) packages, internally developed applications and utilities.
- ❑ Communication/Telephony – Installation, modification, de-installation, or relocation of Phone equipment and services.
- ❑ Generic and Miscellaneous Changes – Any changes that are required to complete tasks associated with normal job requirements.

10.3 Guidelines:

- All changes to the IT infrastructure must be authorized by the IT Steering Committee.
- The IT & Systems Department has overall ownership of the change and is accountable for the change from assessing the initial request, development of the change and implementation of the change to the Production and if appropriate the pre-production environment.

- There will be a single change request process used that includes, as a minimum, a description of and reasons for the change, success criteria, prerequisite changes, appropriate management authorization, requested implementation date and back-out procedures to restore previous conditions.
- There will be a coordinated set of Release Plans (release schedules) for all changes which are not related to faults.
- There will be a formal technical evaluation and audit against standards for proposed changes to assess the test and back-out procedures and the impact on performance and availability.
- Approval will be required from all appropriate functional areas before implementation of a change.
- The IT & Systems department will ensure that all changes have the appropriate sign-offs, as specified on the Change Implementation Form, and preventing the promotion to production status of changes that do not meet this condition.

10.3 Definitions

1. An IT Change is any modification to the software, hardware or environment supporting a business process.
2. Configuration Control records which versions (e.g. version 1.0) of the components are compatible to make up a particular version of the whole system.
3. Control, which means recording the version of a system in production use at any given point in time, and the ability to return a system to that version.
4. Change Management means the processes necessary to ensure that changes have been approved from both business and technical perspectives before they are implemented.

10.4 THE CHANGE CLASSIFICATION

For the purposes of these procedures, changes are defined in terms of four categories namely:

- A change which relates to the development of new program or which alters the functional characteristics of an existing application program and likely come with a cost. This type of change requires both notification and approval by users and IT steering committee/Executive Director before any implementation is undertaken.
- A change which is to fix a fault with the operation of an existing application program. This type of change is required to make the program conform to the most relevant, approved functional specification. In such cases, notification is required advising users that a change to the program is to be made. However, as the change is to ensure the program conforms to a previously agreed functional specification, IT Steering Committee/Executive Director approval for this type of change is not necessary.

- Changes which are of an operational/housekeeping status, typically implemented during normal day-to-day business operations. This will be implemented under a documented procedure. The change will usually be restricted to modifying standing data, and routine systems administration and housekeeping operations. This could be scheduled on a regular basis. IT Steering Committee/Executive Director approval for this type of change is not necessary.
- Change in hardware infrastructure to support smooth running of the business operations. IT Steering Committee approval is necessary for this type of change.

10.5 CHANGE MANAGEMENT PROCESS

There are four major steps within the Change Management Process:

- Change Initiation: - Involved with initiating and logging the change request.
- Change Assessment: - Involved with assessing the business and technical issues from both IT and end users point of view.
- Change Authorization: - Involved with authorization for the change to be progressed or the rejection of the change.
- Change Implementation: - Involved with the planning, scheduling and implementing of changes to any/all of FCMB Pensions IT infrastructure.

Change requests may be initiated by **IT & Systems Department, End-Users,** and **Vendor** and processed according to the following:

1. **Users:** Register a change request through the IT & Systems Department, the requests are to be reviewed regularly by the department. If such request is deemed worthy for development, the Head, IT & Systems department analyze the request and recommend either to proceed (in the case of minor or housekeeping) or seek approval from the IT Steering Committee (for major changes) before any further work is undertaken. If the request is rejected, the department/user requesting is to be informed.
2. **IT Vendors/Service Providers:** They are responsible for their own development methodologies and change management processes. However, any change recommended by the Vendors to FCMB PENSIONS must be supported by documentation from them recommending the change and be formally recorded as supported and approved for implementation. Provided the change is covered under the standard maintenance contract between the Vendor and FCMB PENSIONS and **does not involve additional expenditure** or any special conditions, the need for a separate Change Assessment Form is no longer required.

3. **IT & Systems Department:** Change requests may be requested by the IT & Systems department when it deem fit that such changes will improve operational delivery of the software/hardware infrastructure.

Roles and Responsibilities

The following are the key roles in the Change Management Process. It is important to note that several roles may be performed by one individual (for example, the System Owner may also be the Head of Department), and alternatively several people could fulfil one role (for example, the task of assessing a change might be performed by several people). Roles therefore should not be confused with people.

□ Change Manager

The Change Manager's responsibilities include:

- Managing production and maintenance of the software and core hardware list.
- Coordinating the movement of change requests through the various stages of the Change Management Process.
- Controlling and maintaining the change management and associated documentation and forms.
- Monitoring the Release Plans and resolution of conflicts
- Managing the change approval process
- Advising all stakeholders on the operational status of the change
- Verifying closure of change.

□ Change Developer

The Change Developer is responsible to initiate the change assessment process and manage the development of the change. The Change Developer must be a FCMB PENSIONS employee or contracted vendor.

Responsibilities include:

- Identification of the service or technical need for the change.
- Definition of the success criteria for the change.
- Proposing the change solution in technical terms as appropriate.
- Seeks the approval from the change manager to proceed.

□ Change Implementer

The Change Implementer is responsible to manage the promotion of the change to the pre-production and/or production environments. The Change Implementer's responsibilities include:

- Assisting in planning the technical execution of the change

- Ensuring that those implementing the change have appropriate skills and training and adhere to industry standards and procedures
- Verifying that building and testing of the change has been completed
- Verifying technical function of the change after activation
- Supervising the backing out of the change, if necessary, as specified in the plan documented on the Change Implementation Form
- Must be present during the implementation of the change
- Recording and filing of all documentation, test results and reports associated with the change in a format suitable for, and accessible to, inspection and audit requirements.

❑ **Change Installer**

The Change Installer is the person who is knowledgeable about the operating system and/or database standards and actually performs the installation of the executable into the pre-production/ production system.

❑ **Change Request Priority**

Change request priority is used to indicate an urgency and/or timeframe expected in response to a change request. Four levels of priority defined are:

- Urgent: An acute error in an IT infrastructure causing shutdown or failure or unsatisfactory operation.
- High Priority: A serious error in an IT infrastructure that interferes with the operation of the system but does not actually prevent its use or operation.
- Medium Priority: An error in an IT infrastructure where alternative solutions are available that are acceptable.
- Low Priority: Imperfections in the use of IT based screens, help text, documentation or improvements or suggestions to IT facilities that have no significant effect on the use or operation of the system.

❑ **Business Impact**

Business Impact is used to indicate the impact the change request has on business activities, services and facilities of FCMB Pensions Ltd.

Five categories of business Impact defined are:

- **Unscheduled Outage (Fault only):** A fault has stopped or will stop a component of the application systems and no work-around is available that can be quickly and securely implemented. A fix is required within 24 hours.
- **Workaround Exists (Fault or Change):** A fault has stopped or will stop a component of the application systems, or has significant business implications to the business, and

a work-around is available that can be quickly and securely implemented. The fix is required within 14 days.

- **Scheduled Outage/Scheduled Release (Fault or Change):** The request is to fix a system, network or service fault, or to add new functionality. The request will be implemented in the next planned release.
- **Not Critical (Change or Observation only):** The issue is not critical and has no significant effect on the operation of the system. A fix may be taken up in a future release.
- **None-impact: Change or Observation,** which has no impact on the market.

□ **Validation, and Acceptance**

Once a change has been implemented, a change review must be conducted to determine if the change resulted in the desired outcome. In most cases, this review process might be very brief. For a routine change, where the effect has been small and the results relatively predictable, the review process will be limited to checking that the change has provided the user with the desired functionality.

□ **Monitor Change in Production Environment**

In order to determine whether the deployed change has been effective, it is necessary to monitor the changes in the production environment. For a small change, this may consist of checking on the desired functionality. For larger changes, it might require the monitoring of network and server information, performance data, event logs, or response times.

The actual channel used will depend on the nature of the change, the components of the IT infrastructure that are affected, and the skills and experience of personnel performing the monitoring activity. The Change Manager will typically determine the best channel needed based on the specific change.

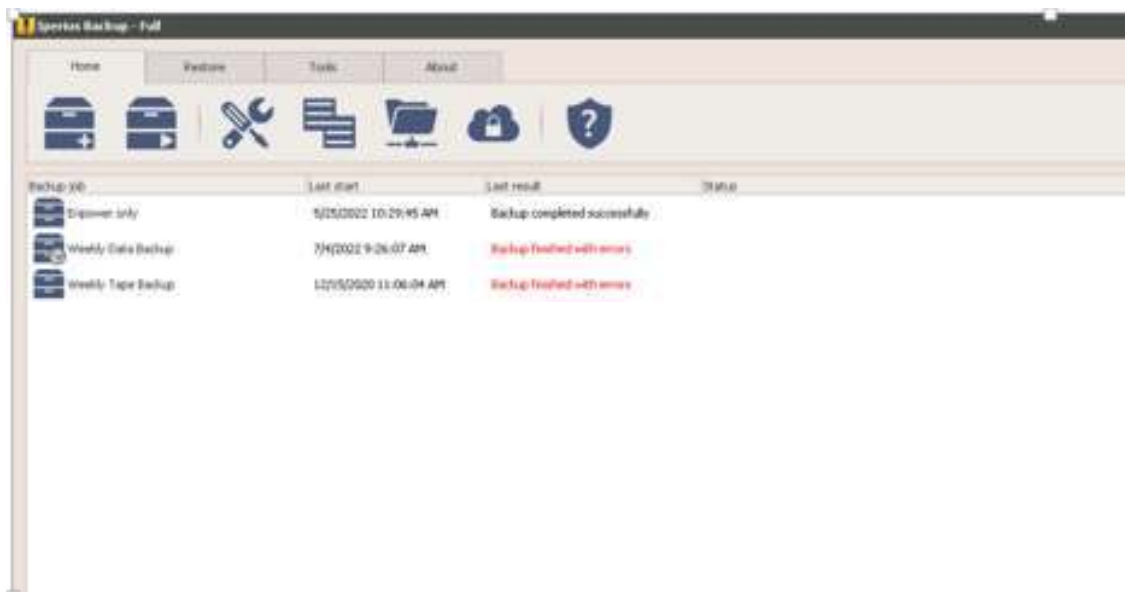
11. TAPE BACKUP PROCEDURE

The tape backup officer is expected to follow the following procedure to ensure effective backup and restoration of the contents on the tape.

This process is of two stages namely the outbound and inbound respectively.

For outbound tapes: The following procedure must be adhered to guarantee records' security and integrity:

- Pick a tape from store and insert into the tape drive in the Data Center.
- Navigate to 172.16.50.40.
- Login using Admin details.
- Search for Iperius Backup Application.
- Right click and run as administrator.
- Click on Home – Weekly Database Backup



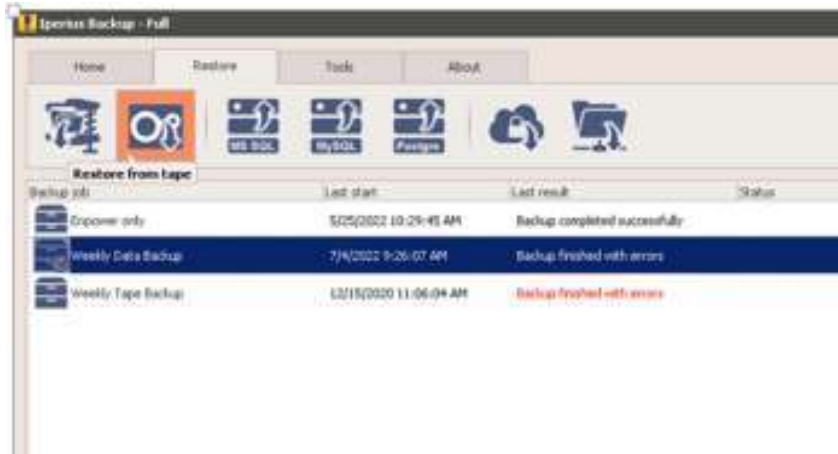
- Right click and select run backup.
- The backup starts and when it finishes, a mail is sent automatically to give the status of the backup.
- The logs can also be checked by right clicking on Backup job and selecting "Show log list"
- Eject backup tape once backup is done successfully.
- Record the backup details in the backup
- Keep the tape in the Gubabi storage.

- Repeat this process every week.

Do a count to make sure you have all expected tapes and that they're ready to be transported after each month. Pack the tapes in the tape case, enclose them in a box and send them to Lagos via Corporate Resources Department. Record the movement in the Movement registers

Backup Restoration: The following procedure must be adhered to guarantee records' security and integrity:

- Simulate data restoration by using any of the tapes already backed up and record in the Logbook.
- Insert the tape that you want to restore.
- Navigate into 172.16.50.40.
- Login using Admin details.
- Search for Iperius Backup Application.
- Right click and run as administrator.
- Click on Restore – restore from tape- select files to be restored and location of restoration.



- Check application and location of restoration to confirm that it was restored successful.

For Inbound Tape:

1. Check the tape received to ensure it tallies with the numbers expected
2. Record it in the movement registers
3. Keep the received tapes in the Gubabi Storage and ready for reuse.

4. Use the Tape Cleaner to clean the Tape head at least once a month.

DATA REPLICATION

Data replication is done from the Head Office to the DR site using the Veeam Backup & Replication software. The software has been configured to replicate the servers and databases at the end of each day.

At the scheduled time, the software replicates from the SAN in the Head Office to the SAN in the DR site.

Checks are carried out once a week on the DR SAN to ensure that the replicated data is complete and accessible.

12. EVENING/CLOSING TASK

At the close of work for each day, IT department will perform inspection of Data Centre facilities and Application services to ensure that schedule services and report run as expected.

The Following task must be performed accordingly:

- Application Check
- Login remotely to the servers
- Check the status of all 'Services'
- Check the status of all applications
- Check the status of all external links (branch portal, member self-service, company website)
- Log out

Check the status of schedule SMS and E-mail Services

- Check to ensure that SMS and Email services are up and running so that it can pick up and run at scheduled time and frequency.

Workstation Management Procedure

Overview

Workstation Management provides technical support for State-owned personal computers (PC). Workstations receiving standard desktop support are managed with standard processes, tools, and policies. Remote administration tools are used whenever possible to minimize interruptions and provide faster service. Support provided by Workstation Management Technicians include: installations, configurations, connections, maintenance, troubleshooting, and repair of computers, accessories and peripherals

Standard Features

This section describes the standard features of the Workstation Management service. Where applicable, customer options are noted, along with feature limits and the responsibilities of FCMB Pensions Limited.

Operating Systems

The Operating System (OS) links the workstation hardware resources (e.g., hard drive, processor and memory), user input/output devices (e.g., keyboard, mouse and monitor), and the workstation software applications (e.g., Microsoft Office, web browser, etc.). The primary supported operating system by FCMB Pensions Limited is the Microsoft Windows client operating system; more specifically Windows 10 and Windows 11. All standard workstations will have Windows 10/11 Professional installed, because they have to be joined to the domain.

Workstation Hardware Inventory

The workstation hardware inventory process involves tracking desktop and laptop assets through their life cycle and facilitating their transition through different life cycle phases (e.g., acquisition through disposal). The process collects and maintains the following list of information:

- Hardware manufacturer
- Make/Model
- Serial number
- Asset number
- Current assignee
- Location
- Current operating system

Workstation Software

To ensure laptops and desktops are deployed consistently, standard operating system builds (including the installation of the workstation client operating system and standard software) will be

used. These installations can be automated and greatly reduce the time required to deploy a workstation. Software is classified into the following categories (with additional information in the sections below):

- **Required software** – Mandatory software installed on all workstations. (Antivirus, Malware/spyware protection, local firewall (e.g., Windows Firewall), hard drive encryption (e.g., Microsoft Bitlocker) etc.
- **Standard software** – Provides a common application set to all end users (Microsoft Office productivity suite (e.g., Microsoft Office 2013 including: Access, Excel, InfoPath, One Note, Outlook, PowerPoint, SharePoint Workspace, and Word) Microsoft .Net Framework, PDF Reader (i.e., Adobe Reader), Web Browser (i.e., Internet Explorer) etc.

Unique/core software

Some business units or end users may require unique or “one-off” additional software. The installation of such software is permissible where the business unit provides the necessary installation media and license key(s) e.g. Microsoft dynamics Business central.

Workstation Backups and Restores

Workstation backup and restore is the process of copying data preemptively for the specific purpose of restoring that same data. Data is often restored due to hardware failure, accidental deletion or corruption of data, a previous version is desired, or the device is lost or stolen. It is recommended that files be stored in centralized (non-local) location such as a file server. This enables end users to quickly access data after a hardware failure or if the device is lost or stolen; as they do not need to wait for data restoration.

File Server

A file server provides a centralized location for shared disk access, i.e. shared storage of computer files (such as documents, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network. File servers provide two types of file shares:

- **Personal** – File shares assigned to a specific end user for their sole use
- **Shared** – File shares assigned to a Department with permissions granted to members of that department alone.

Laptops/ Workstation Standardization Practice

- Users cannot install or download software applications and or/executable files to any Desktop or laptop computer without a prior authorization.
- Users can not change endpoints settings.

- Users can not update the system's timestamp.
- Antivirus is installed on all endpoints. This is updated from the EPO antivirus server whenever an update is available.

APPENDIX

IT Complaint Form

Complainant Name	
Department	
Date	
Signature	

Complain	
S/No	Details

FOR IT & System Department Only

Suggested Priority		
<input type="radio"/> High	<input type="radio"/> Medium	<input type="radio"/> Low
Complain Type		
<input type="radio"/> Software	<input type="radio"/> Hardware	<input type="radio"/> Operation

Analysis:

Recommendation:

Action Taken:

Signature & Date:

IT Request Form



Staff Name	
Department	
Date	
Staff Signature	
HOD comment	
HOD Signature	

Qty	Request Description	Purpose

For IT & System Department Only

Request Type

- Software
- Hardware
- Consumables

Date of Last Purchase.....

Request Analysis

Request Cost

Head of Department
Signature

.....
Date

Approval

.....
Signature

.....
Date

Comment:



IT Change Request Form


1.) REQUESTER - GENERAL INFORMATION			
Type of CR	<input type="checkbox"/> Enhancement	<input type="checkbox"/> Defect	<input type="checkbox"/> New
Software/Hardware Name			
Requester Name			
Requester Department			
Brief Description of Request			
Date Submitted			
Date Required			
Priority	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High <input type="checkbox"/> Mandatory
Benefits of Change Request			
Other Services Impacted			
Attachments/References	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
HOD Approval Signature		Date Signed	

2.) PROJECT MANAGER (Head, IT & Systems Department) - INITIAL ANALYSIS		
Duration Impact		
Business Impact		
Cost Impact		
Comments		
Recommendations		
Attachments/References	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Approval Signature		Date Signed

3.) AUDIT REVIEW			
Review Date			
Reviewed Decision			
Comment			
Signature		Date Signed	

4.) CHANGE MANAGEMENT / IT STEERING COMMITTEE – DECISION					
Business Impact	<input type="checkbox"/> Outage	<input type="checkbox"/> Workaround exists	<input type="checkbox"/> Scheduled	<input type="checkbox"/> Not critical	<input type="checkbox"/> No impact
Decision	<input type="checkbox"/> Approved	<input type="checkbox"/> Approved with Conditions	<input type="checkbox"/> Rejected	<input type="checkbox"/> More Info	
Decision Date					
Decision Explanation					
Conditions					
Approval Signature		Date Signed			

USER CREATION ACCESS

 IT & SYSTEMS DEPARTMENT	USER CREATION ACCESS	CODE REFERENCE: ICT-UCA0001

STAFF NAME:

DEPARTMENT:

HEAD OF UNIT:

DATE:

PLEASE TICK

APPLICATIONS	GRANT ACCESS	REVOKE ACCESS
MS DYNAMICS 365		
BACK OFFICE		
BRANCH PORTAL		
BENEFIT PROCESSING PORTAL		
DOCUWARE		
MONEYPLUS (FUND ACCOUNT)		
MONEYBOOK (INVESTMENT)		
HR WORKPLACE (CR)		
SAGE EVOLUTION (ACCOUNTS)		
QLIKVIEW		
Others		

USER ACCESS LEVEL.....

.....

PURPOSE.....


.....

HOD Signature.....

ED OPERATIONS (COMMENT/APPROVAL):-.....

I.T COMMENT:-.....

DATABASE ACCESS GRANT FORM

 IT & SYSTEMS DEPARTMENT	DATABASE ACCESS GRANT FORM	CODE REFERENCE: ICT-UCA0002

STAFF NAME:

DATE:

PLEASE TICK

APPLICATIONS DATABASE REQUIRED	GRANT ACCESS	REVOKE ACCESS
MS DYNAMICS 365		
REG AGENT (RPC'S)		
MONEYPLUS (FUND ACCOUNT)		
MONEYBOOK (INVESTMENT)		
HR WORKPLACE (CR)		
SAGE EVOLUTION (ACCOUNTS)		
OLIKVIEW		
IVR		

USER ACCESS LEVEL.....

.....

PURPOSE.....

.....

Head IT, Comment:..... Head IT, Signature

	IT & Systems Dept.	IT EQUIPMENT REPAIR FORM	Code: ICT-COL-003

Complainant Name	
Department	
Date	
Signature	
HOD's Signature	

Equipment Detail	
S/No	Details




<u>FOR IT & System Department Only</u>		
Suggested Priority		
<input type="radio"/> High	<input type="radio"/> Medium	<input type="radio"/> Low
Repair Cost:		

Head IT & Systems:
Signature Date

ED, Operations & Services:
Signature Date

MD, CEO:
Signature Date

APPROVAL PAGE

IT & SYSTEMS DEPARTMENT	
Designation	
Head, IT & Systems Department	Lukman Yusuf Sign:  Date: 21/07/19
Executive Director, Operations & Services	Christopher Bajowa Sign:  Date: 18/4/19
Managing Director/CEO	Misbahu Yola Sign:  Date: 18/07/19
Chairman, Board Risk Management Committee	Suzanne Iroche Sign:  Date: 30/7/19
Chairman, Board of Directors	Ladi Balogun Sign:  Date: 20/7/19