
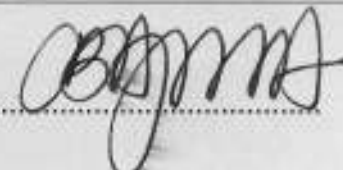




DEPARTMENT	IT & SYSTEMS
TITLE OF DOCUMENT	IT & SYSTEMS POLICY DOCUMENT
Author / Prepared by:	HEAD, IT & SYSTEMS DEPARTMENT
Date & Signature of Author	Date: 19/10/2023 Sign: 
APPROVED BY:	
Managing Director & CEO	Date: 19/10/2023 Sign: 
Chairman Risk Committee	Date: 19/10/2023 Sign: 
Board Chairman	Date: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

Date of Last Approval:	28/04/2019	Date Policy Will take effect:	Immediate
Title of Manual	IT & Systems Department Policy Document		
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 Content

	Page
Policy Code: FPL_IT_SP_01	Policy Name: IT Policy Life Cycle 5
Policy Code: FPL_IT_SP_02	Policy Name: Information Security..... 7
Policy Code: FPL_IT_SP_03	Policy Name: Password Security11
Policy Code: FPL_IT_SP_04	Policy Name: Email and Instant Messaging15
Policy Code: FPL_IT_SP_05	Policy Name: Mobile Device Security Policy 18
Policy Code: FPL_IT_SP_06	Policy Name: Intranet Usage 20
Policy Code: FPL_IT_SP_07	Policy Name: Website Management Policy 22
Policy Code: FPL_IT_SP_08	Policy Name: Internet Usage..... 25
Policy Code: FPL_IT_SP_09	Policy Name: Remote Work Policy 27
Policy Code: FPL_IT_SP_10	Policy Name: Software Acquisition & Usage & Software Licence Management Policy 30
Policy Code: FPL_IT_SP_11	Policy Name: IT Hardware Acquisition Policy..... 35
Policy Code: FPL_IT_SP_12	Policy Name: Equipment Obsolescence/Disposal Policy 43
Policy Code: FPL_IT_SP_13	Policy Name: Innovation Management Policy 46
Policy Code: FPL_IT_SP_14	Policy Name: Patch Management Policy..... 50
Policy Code: FPL_IT_SP_15	Policy Name: Vendor Performance Management.....54
Policy Code: FPL_IT_SP_16	Policy Name: Cloud Computing Management.....60
Policy Code: FPL_IT_SP_17	Policy Name: Software Development Policy 62
Policy Code: FPL_IT_SP_18	Policy Name: Backup & Recovery Policy74
Policy Code: FPL_IT_SP_19	Policy Name: Database Management Policy735
Policy Code: FPL_IT_SP_20	Policy Name: Data Usage Policy..... 79
Policy Code: FPL_IT_SP_21	Policy Name: Data Breach Incident Management Policy 81
Policy Code: FPL_IT_SP_22	Policy Name: Active Directory Domain Policy 85
Policy Code: FPL_IT_SP_23	Policy Name: Data Centre Access Control Policy..... 87
Policy Code: FPL_IT_SP_24	Policy Name: Vulnerability Management Policy 90
Policy Code: FPL_IT_SP_25	Policy Name: CCTV Policy.....92
Policy Code: FPL_IT_SP_26	Policy Name: Laptop Management94

FCMB Pensions Limited

IT Policy Document

This policy document is intended to encompass the applications of Information Technology in all areas: departments, support services and all other organisational structures. Therefore, all members of staff are stakeholders as well as the company's clients.

It is also a document that guides IT service delivery in its widest sense:

- Systems - to support corporate, departmental and business operational needs of the company.
- Services - help, support, training, systems development, business and systems analysis, and project management
- Infrastructure - networking, computing environments and machinery

PURPOSE

- 1) To promulgate the company's policies and standards for information technology.
- 2) To provide guidelines to assist the company in the development of short- and long-term plans for their information systems;
- 3) To provide guidelines and procedures for the procurement and maintenance of information technology assets;
- 4) To provide standards to ensure the security of information technology assets of the company.

AUTHORITY

Regulatory bodies – National Pension Commission, require the company to develop policies and standards for its information technology.

These policies document were developed by IT & Systems Department of FCMB Pensions. Subsequently, any of the company's arm or officer that uses the equipment or services of the ITSD must adhere to the regulations, standards, practices, policies and conventions that are codified herein.

DEFINITIONS

- **ITSC** – Acronym for IT Steering Committee.
- **ED, OP&S** – Acronym for Executive Director, Operations & Services
- **ITSD** - Acronym for Information Technology & Systems Department.
- **Policy** - A high-level statement of purpose used to guide and determine present and future decisions and actions.
- **Standard** - A structure which has been established to serve as a model.

ADMINISTRATION

An employee of the ITSD who has been appointed as the Head, IT & Systems will coordinate the administration and implementation of Information Technology Policies, Standards and Procedures.

Coordination will involve communication of any intended change to ITSC with opportunity for review of the modified or new policy, standard, or procedure.

IT Policy Life Cycle Process

1. Identification, Planning and Initiation

- a. Identify compelling need for new or updated policy/guidance. Drivers may include new regulatory requirements, technology developments, operational needs, and identification of current issues or gaps.
- b. Request may come from any unit, or department who recognizes the need for modifications and/or additional information to the policies. Such may be submitted in writing to the ITSC.
- c. Determine whether the need should be satisfied by a policy, guideline, or standard
- d. Identify sponsorship, stakeholders, and their relevant roles
- e. Develop high level implementation impact analysis
- f. Obtain approval to proceed with draft policy (or guideline, standard)
- g. Prioritize and schedule policy work

2. Development, Review, and Approval

- a. Draft initial policy (guideline, standard)
- b. Distribute to IT Steering Committee for initial review and input
- c. Incorporate initial feedback
- d. Distribute to a BOD for review and input
- e. Review and, where appropriate, incorporate feedback
- f. Obtain approval

3. Rollout

- a. Announce guidance (policy standard, guideline)
- b. Initiate implementation activities
- c. Determine ongoing review cycle (default review cycle is annual)
- d. Upload the document for reference via the Intranet Web Page at <https://web.fcmbpensions.com/intranet/internalManuals.aspx> for all staff. Additionally, a printed copy of the ITSP shall be made available to any staff of the company approved by Management.
- e. The company reserves sole ownership of the IT SP, and under no condition shall this document be reproduced, copied or distributed outside the company without appropriate approval from the Management.

4. Compliance, Review and Maintenance

- a. Monitor compliance and effectiveness of implemented guidance
- b. Review and implement modifications per annual review cycle (last revision and review dates shall be posted on each policy).

5. Policy Retirement

- a. As part of the maintenance and review process, policies, standards, and/or guidelines may be identified as out-of-date or no longer needed. They will be retired via the same process by which they were approved.

Objective: Provide guidelines that protect the data integrity of FCMB Pensions information systems.

Applies to: All employees

Key guidelines:

By information security we mean protection of FCMB Pensions' data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- To establish a company-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of FCMB Pensions data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of FCMB Pensions and allow the company to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to the regulator, business partners and worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- FCMB Pensions will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the company's data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.

The IT & Systems Department must ensure that:

- The information security policy is updated on a regular basis and published as appropriate.
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Each department must appoint a person responsible for security, incident response, periodic user access reviews, and education of information security policies for the department.
- Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis.

- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by FCMB Pensions.

User Access Management

Objective: To prevent unauthorised access to information systems.

- User registration: There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.
- Privilege management (user access granting/revocation): The allocation and use of privileges shall be restricted and controlled using the 'user access creation' form.
- User password management: The allocation of passwords shall be controlled through a formal management process.
- Where possible and financially feasible, more than one person must have full rights to any FCMB Pensions owned server storing or transmitting high risk data.
- Access to the network, servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, biometrics, or other recognized forms of authentication.
- Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT & Systems Department.
- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT & Systems Department.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.
- Transferred employee access must be reviewed and adjusted as found necessary.

- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Note: User Access Procedure is contained in the Standard and Procedures Document (8 – 9)

Virus Prevention

- The wilful introduction of computer viruses or disruptive/destructive programs into the company environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.
- FCMB Pensions has in place McAfee ePolicy Orchestrator ver. 8.8 - an Enterprise Anti-virus, with automatic updates of the DAT files.

Intrusion Detection/ Firewall review

- Intruder detection must be implemented on all servers and workstations containing data classified as high or confidential risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- An auto generated report for virus malware detection and security audit report is sent from the Sophos XG230 device to System Administrator, IT Auditor, and the Risk Manager on a daily basis.
- Firewall auto generated report is reviewed and documented by the IT security personnel.
- Intrusion detection tools should be installed where appropriate and checked on a regular basis.

Information security awareness should be organised quarterly to enable staffs have the knowledge to be security conscious while using the company's it infrastructure.

Note: A detailed Information Security Policy is attached in Appendix 1

Objective: Provide guidelines in appropriate management of business passwords to maintain adequate security and integrity of all of FCMB Pensions business systems.

Applies to: All employees with authorized access to Computer Systems/Network facilities.

Key guidelines:

Maintaining security of FCMB Pensions' business applications, software tools, email systems, network facilities, and voice mail are critical to providing data integrity and stability of our systems.

Passwords are provided to limit access to these company assets on an as needed basis.

- FCMB Pensions provides access to network, electronic mail and voice mail resources to its employees in support of the FCMB Pensions' mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
- It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by FCMB Pensions.
- The IT & Systems Department will establish guidelines for issuing new passwords, deleting passwords as required, and allowing employees to change their passwords.
- Although FCMB Pensions strives to manage a secure computing and networking environment, the company cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.
- New employee passwords and changes must be requested by a Manager. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing FCMB Pensions systems.
- A network manager must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.
- The IT & Systems Department will delete all passwords of exiting employees upon notification from Human Resources.
- System administrators and users assume the following responsibilities:
 - a. System administrator must protect confidentiality of user's password.
 - b. User must manage passwords according to the Password Guidelines.
 - c. User is responsible for all actions and functions performed by his/her account.

- d. Suspected password compromise must be reported to the Head-Information Technology immediately.

Password Guidelines

Select a Wise BUT Complex Password

To minimize password guessing:

- a. Do not use any part of the account identifier (username, login ID, etc.).
- b. Use 8 or more characters.
- c. Use mixed alpha and numeric characters.
- d. Use two or three short words that are unrelated.

Keep Your Password Safe

- a. Do not tell your password to anyone.
- b. Do not let anyone observe you entering your password.
- c. Do not display your password in your work area or any other highly visible place.
- d. Change your password periodically (every 3 months is recommended).
- e. Do not reuse old passwords.

Additional Security Practices

- a. Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.
- b. A Frequent sensitization awareness on our password policy will be carried out at the head office, intranet and via mail where necessary to staff off location on password security practices

Complexity: Within the limits of the operating system or application, passwords must:

- Contain a minimum of Eight (8) characters.
- Contain at least three (3) out of the following four (4) types of characters:
 - o Upper case characters (A-Z).
 - o Lower case characters (a-z).
 - o Numerical characters (0-9)
 - o Special characters (! @ # \$ % ^ & * () _ + | ~ - = \ ' { } [] : " ; ' < > ? , . /) .

In addition, users should not use passwords that contain:

- Words found in a dictionary (English or foreign)
- Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software.
- Identifiable personal information, names of family, birthdays, addresses, phone numbers, etc.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Words preceded or followed by a digit (e.g., secret1, 1secret)
- Words spelled backwards.
- Slang, dialect, or jargon words from any language.

Management: The following password management practices must be followed and where technically possible, system controls must be configured as follows:

- All user-level passwords (e.g., email, web, desktop computer, Dynamics 365 Admin & Moneytor IBS, Sage Pastel etc.) must be changed at least every 90 days.
- Prevent password reuse with a history of the last 6 passwords.
- Maximum password age of 90 days.
- Minimum password age 3 days.
- Password complexity checking.
- Account lockout after 3 sequential invalid logon attempts.
- Account lockout duration for a minimum of 15 minutes.
- Must not store passwords in clear text or in any easily reversible form.

Protection: Users are responsible for the following:

- Passwords should be memorized and never be written down or stored on-line (including Mobile phones, Palm Pilots or similar devices).
- Do not reveal your personal password to ANYONE, including administrative assistants or management.
- Group passwords must be tightly managed and facilitate individual accountability; however, ultimate responsibility resides with the owner.
- Never reveal a password electronically, such as an email message.
- Do not talk about a password in front of others.
- Do not use the same password for FCMB Pensions accounts as for other non-FCMB Pensions access (e.g., personal ISP account, option trading, benefits, etc.).
- Do not use the "Remember Password" feature of applications (e.g., Mozilla Firefox, Outlook, Netscape Messenger, Windows, Internet Explorer, etc.).
- Again, do not write passwords down and store them anywhere in your office.

- (Consider simultaneously resetting all BUSINESS system user accounts to the same password to facilitate easier memorization).
- If an account or password is suspected to have been compromised, report the incident to the IT & Systems Department and change all passwords.
- Avoid others watching you type your password (shoulder surfing).

Objective: Provide appropriate guidelines for productively utilizing the FCMB Pensions' email system and instant messaging technology that protects the employee and company while benefiting our business.

Applies to: All employees

Key guidelines: FCMB Pensions has established this policy with regard to the acceptable use of company provided electronic messaging systems, including but not limited to email and instant messaging.

Email and instant messaging are important and sensitive business tools. This policy applies to any and all electronic messages composed, sent or received by any employee or by any person using company provided electronic messaging resources.

FCMB Pensions sets forth the following policies but reserves the right to modify them at any time in order to support our company:

General

- FCMB Pensions provides electronic messaging resources to assist in conducting company business.
- All messages composed and/or sent using FCMB Pensions provided electronic messaging resources must comply with company policies regarding acceptable communication.
- FCMB Pensions prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- Upon termination or separation from the company, FCMB Pensions will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Each employee will be assigned a unique email address that is to be used while conducting company business via email.
- Employees authorized to use instant messaging programs will be advised specifically on which instant message program(s) are permissible.
- Employees authorized to use instant messaging programs will be assigned a unique instant messaging identifier, also known as a buddy name, handle or nickname.

- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify a manager or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Ownership

- The email/electronic messaging systems are FCMB Pensions' property. All messages stored in FCMB Pensions provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of FCMB Pensions. Electronic messages are NOT the property of any employee.
- FCMB Pensions reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- FCMB Pensions reserves the right to alter or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the company. Employees may use these identifiers only while employed by the company.

Confidentiality

- Messages sent electronically can be intercepted inside or outside FCMB Pensions and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.
- Employees are prohibited from unauthorized transmission of company trade secrets, confidential information, or privileged communications.
- Unauthorized copying and distribution of copyrighted materials is prohibited.
- Employee should desist from sending unsolicited mails to any mailbox, except in the course of doing business or giving instruction, with the official e-mails.
- Employees must use a standard mail signature deployed on MS outlook.

Security

- FCMB Pensions employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on company provided computer equipment.
- Although FCMB Pensions employs anti-virus software, some virus infected messages can enter the company's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
 - Be suspicious of messages sent by people not known by you.
 - **Do not open attachments** unless they were anticipated by you. If you are not sure, **always verify** the sender is someone you know and that he or she actually sent you the email attachment.
 - Disable features in electronic messaging programs that automatically preview messages before opening them.
 - Do not forward chain letters. Simply delete them.
- FCMB Pensions considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use FCMB Pensions provided email addresses when posting to message boards.
- Disclaimer should be developed to be appended to all outgoing mails.
- All confidential attachments to outgoing mails should be appropriately encrypted.

Inappropriate Use

- Email or electronic messaging systems shall not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- FCMB Pensions provided electronic messaging resources shall not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.

Policy Code: FPL_IT_SP_05

Policy Name: Mobile Device Security Policy

Objective: To provides guidelines for securing and appropriate access to the company's software application on both privately owned and corporate mobile devices, such as smart phones and tablet.

Applies to: All employees

Key guidelines: Mobile devices, such as smart phones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. However, users of such devices often give greater weight to their own rights on the device than to their employer's need to protect data, hence the need for this policy to guide its usage.

General

Mobile devices represent a significant risk to information security and data security, as such, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

FCMB Pensions has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of policy guiding safe use of mobile devices.

Scope

All mobile devices, whether owned by FCMB Pensions or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smart phones and tablet computers.

- Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted and authorized by the Executive Director, Operations & Services.

Policy Details

- Device Requirements: Devices must be Windows platform, Android, Blackberry or Apple devices
- Devices must be configured with a secure password that complies with FCMB Pensions' password policy. This password must not be the same as any other credentials used within the organization except for email.

- With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

User Requirements

- Users must contact IT & System department for email configuration on their mobile device(s)
- Users must report all lost or stolen company owned devices to the IT & Systems department immediately.
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system.
- If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify IT & Systems department immediately.
- Users must not use corporate workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.
- If a user suspects that unauthorized access to company data has taken place via a mobile device, such user must report the incident to the IT & Systems department immediately.
- In case of termination/resignation from FCMB Pensions, all company owned device must be return to IT & Systems department while user account must be deactivated upon instruction from Corporate Resources department to prevent further synchronization with user's mobile device(s).
- Users must not load pirated software or illegal content onto company owned devices.
- Applications must only be installed from official platform-owner approved sources.
- Installation of application from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact the IT & Systems department.
- Devices must be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked for weekly and applied at least once a month.
- Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware/virus protection and which does not comply with corporate policy.

Objective: Provide guidelines for the appropriate use of FCMB Pensions' Intranet to improve the productivity and effectiveness of our staff and company and to maintain security of our Intranet assets.

Applies to: All employees

Key guidelines: FCMB Pensions Intranet is a proprietary web-based source of content, knowledge base, and process tool for our internal employees and managers. Security measures have been established to allow FCMB Pensions employees and managers access to appropriate sections of FCMB Pensions Intranet to assist in their efforts in conducting our business.

- All full-time employees of FCMB Pensions are approved for access to the company Intranet. Part time employees and contracted resources must have management approval for Intranet access.
- Intranet security passwords are the responsibility of each individual authorized to access the Intranet. Passwords are not to be shared, swapped, or given out in any form. Keep passwords hidden from view and protect the integrity of your FCMB Pensions' employee information.
- Technology Solution Lead and Brand Champions are responsible for setting the goals and objectives for FCMB Pensions' Intranet, determining priorities for adding new content, and for maintaining the integrity of the Intranet site.
- Technology Solution Lead and Brand Champions are also responsible for defining, creating, and maintaining consistent format for all web sites and pages developed for the Intranet regardless of original department source.
- Each of FCMB Pensions' operational and support departments will be represented in the Intranet Steering Committee to provide content and processes that enhance employee knowledge and productivity. Submit feedback and suggestions to your department representative.
- All content residing on the FCMB Pensions' Intranet is the property of FCMB Pensions.
- Maintenance of the Intranet is an assigned role established by the Head, IT.
- FCMB Pensions will provide a central Home Page access that will be the employee's main entry point into the company's Intranet as follows:
- Departments may include links in department sites/pages for downloading documents and files in the following formats:

- Microsoft Excel
 - Microsoft Word
 - Microsoft Access
 - Microsoft PowerPoint
 - Adobe PDF
 - Images and video files approved by the IT Steering Committee
- Downloaded files from the Intranet are considered proprietary information of FCMB Pensions and should be treated as such.
 - FCMB Pensions' Intranet represents an ongoing reflection of FCMB Pensions. It is every employee's right and obligation to provide input that constantly improves the accuracy of all content and includes new material for consideration that enhances your experience with FCMB Pensions.

Guidelines for adding contents on the Intranet

The following steps are general guidelines for adding new Intranet content:

- Review Intranet Guidelines and Policy.
- The head of department comes up with a proposed content(s)
- The content is passed to IT & Systems Department for review.
- The IT & System Department pass it to the IT Steering Committee for approval
- IF NOT APPROVE: The IT & Systems Department suspend the implementation
IF APPROVED: Continue to the next step.
- Sketch out information and proposed organization of the contents.
- Assemble and develop content required for each page.
- Maintain content and hyperlinks of the new content according to Intranet guidelines.

Objective: Provide guidelines for the appropriate use of FCMB Pensions' Internet to improve the productivity and effectiveness of the company's service delivery.

It is aimed to:

- a. protect, promote and enhance the company's brand and image;
- b. enhance the customer experience and satisfy the enquiries of those visitors and users of the site, by offering engaging content, focused upon end user needs;
- c. reduce complexity and duplication of website content through website management and maintenance efforts

Applies to: This policy covers the website found at the following URL:
<https://www.fcmbpensions.com>.

We use the services of a third party website developer to host the website and develop it when required. Appropriate agreements are in place to ensure optimum quality control measures.

Security

The IT & Systems department, the E-Business unit and the website developers are the only parties who have access to the website.

Key Purpose:

This policy aims to clearly explain the roles and responsibilities of all parties involved in online content management ensure best practice in content management and usability principles are established and adopted by FCMB Pensions; outline processes for online content review, maintenance and development of FCMB Pensions website by:

- Ensuring content is up to date;
- Ensuring content does not infringe copyright;
- Specifying conditions for downloading material;
- Ensuring compliance with the PENCOM REFORM ACT 2014;
- Overseeing linking arrangements;
- Ensuring posting of a privacy notice explaining how any data collected from visitors will be managed by the practice.

Collection, Utilisation and Security of Data

Data Collection: Without limitation, any of the following Data may be collected through our online live chat:

- Name;
- Contact information such as email addresses or telephone numbers;
- PIN

This is to allow us to identify the true identity of our online client and be able to serve them better.

Web content guidelines and standards

The criteria below have been established to ensure that content on the Company's website continues to be relevant and appropriate for the medium and the targeted audience.

All content must be approved by the IT Steering committee or the Compliance Officer as being appropriate for the intended audience before it is included on the web content

General Contents: The Website content must align with the company's policy and criteria set by National Pension Commission before it will be approved and published: some of these are:

- minimum information provision, for example, "About us" information,
- Service information,
- Contact details
- User self-service, e.g. Unit price history, branch portal, downloading forms or publications

News articles: News articles will only be published on the website if they are timely and relevant will assist users, or keep them informed of recent events.

Style guide compliance: Content must comply with the standards set out in the Online writing style guide, online writing accessibility, including documents and images structure metadata online presentation and PENCOM guideline for website where applicable.

Homepage content: Requests for material to appear on the homepage of the other than news articles should be directed to Head, IT & Systems. Content will only be considered for placement on the homepage if it: is aligned with overall website direction and is relevant to either the majority of

users or an important target audience focuses on the immediate need to communicate information to users.

Adding or moving a section or landing page: Requests for adding a new section or moving one section to another place must be directed to the Head, IT & System. Requests will only be considered if adding or moving the section/landing page: is of demonstrated benefit to users – for example, improving the discoverability of information is aligned to organisational priorities.

Publishing images: Images will only be published on the website if they: are optimised for the web and are relevant, compelling and add value, comply with accessibility standards and do not infringe copyright.

Linking to external websites: It is best practice to provide links to external websites to avoid duplication of information, and to provide access to the most accurate source of information. External websites must only be linked to where:

- valuable content is being offered the information provided is relevant,
- Credible and accurate the information provided does not conflict with information or advice published on the FCMB Pensions website. In general, links to the following are acceptable: National Pension Commission, Pension Fund Custodian and other partner organisations.
- Does not implies commercial advertisement

All contents on the website must be available to all users, therefore no password protection or limiting access of documents is permitted. PDF documents should not have inbuilt security applied to prevent content copying unless there is a strong and valid business need for such. (Applying such security reduces the efficacy of the search facility).

Content review and maintenance

The IT and Systems department must undertake a regular review process to ensure that the company's website content is kept up to date, accurate, relevant and adhere to PENCOM's guideline.

Objective: Provide appropriate guidelines for accessing and utilizing the Internet through FCMB Pensions' network.

Applies to: All employees with authorized access to Internet services

Key guidelines: Internet services are authorized to designated employees by their manager to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the company must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

General

- Internet accounts are approved for designated employees by FCMB Pensions IT Steering Committee to provide tools that assist in their work. Exceptions from the designated employees shall be on the recommendations of the HOD and approved by the IT steering Committee
- Each individual is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of FCMB Pensions and support the company's goals and objectives.
- These services must support legitimate, mission related activities of FCMB Pensions and be consistent with prudent operational, security, and privacy considerations.
- IT Steering Committee will take responsibility for all web site and format presentation to reflect the FCMB Pensions' mission and in supporting company and departmental objectives.
- FCMB Pensions has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
- FCMB Pensions reserves the right to restrict access to the Internet by employees, or restrict access to such days and time period as the company might deem necessary.

Inappropriate Use

- The following uses of company provided Internet access are not permitted:
 - a. To access, upload, download, or distribute pornographic or sexually explicit material
 - b. Violate state, local, or federal law
 - c. Vandalize or damage the property of any other individual or organization
 - d. To invade or abuse the privacy of others
 - e. Violate copyright or use intellectual material without permission
 - f. To use the network for financial or commercial gain
 - g. To degrade or disrupt network performance
- No employee shall use FCMB Pensions facilities knowingly to download or distribute pirated software or data. The use of file swapping software on FCMB Pensions computers and networks is prohibited.
- No employee shall use FCMB Pensions' Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- No employee shall use the Internet facilities for unofficial purposes during official hours.

Policy Code: FPL_IT_SP_09

Policy Name: Remote Work Policy

Objective: To provide guidelines on appropriate use of remote access capabilities to FCMB Pensions' network, business applications, and systems.

Applies to: All employees, vendors and agents with a personal or company owned computer or workstation used to connect to FCMB Pensions' network.

Key definition:

This is the ability of an individual to work outside the office using a computer system.

Key guidelines:

- The purpose of this policy is to define standards for connecting to FCMB Pensions network from a remote location outside FCMB Pensions.
- These standards are designed to minimize the potential exposure to the company from damages that may result from unauthorized use of the company resources. Damages include the loss of sensitive or confidential company data, intellectual property.
- This policy applies to remote access connections used for/or on behalf of FCMB Pensions, including reading or sending email and viewing Intranet web resources.
- It is the responsibility of the company employees, contractors, vendors and agents with remote access privileges to FCMB Pensions' corporate network to ensure that their remote access connection is given the same consideration as the on-site users.

9.1. Employee Working from Home/Remotely

- a. Secured remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong pass phrases.
- b. At no time should FPL employee provide his/her login or email password to anyone, not even a family member.
- c. FPL employees with remote access privileges must ensure that the company owned or personal computer, which is remotely connected to the company's corporate network, is not connected to any other network at the same time.
- d. The employees with remote access privileges to the company's corporate network must not use non company email accounts (i.e., Yahoo, Hotmail, gmail, etc), or other external resources to conduct the company business, thereby ensuring that official business is never confused with personal business.

- e. All hosts that are connected to FCMB Pensions internal networks via remote access technologies must use the most up-to-date anti-virus software.
- f. Third party connections must comply with requirements defined by the IT & Systems Department.
- g. Personal equipment that is used to connect to FCMB Pensions networks must meet the requirements of the company-owned equipment for remote access.

9.2. Employee Remote Access Procedure

- a. The HODs are expected to forward Management approval for remote work to IT&S.
- b. IT&S to configure the corresponding workstation for remote access
- c. IT&S to provide remote login details to respective staff.
- d. Employee to complete work from home form and obtain necessary approval.

9.3. Approval Process for Remote Vendor Access

All task/resolution that required vendor's remote support must adhere strictly to the guidelines contained herewith.

- Department/user requiring support must route such through IT & Systems and must be approved by either the HOD or the Systems Administrator.
- The assigned IT staff must reach out to the concern vendor through any of the following communication channels; email, mobile call or Help ticket.
- At the agreed time, the IT staff will login to a dedicated Desktop in the department, launch the Remote Application and send the access code to the vendor.
- The vendor connects through this access code while the IT staff watch and support the vendor as the need arise.
- The vendor informs the IT staff of a successful/unsuccessful resolution and the concerned department or IT staff will confirm the status.
- If successful, the resolution will be transfer to the production environment and the remote connection is terminated.
- If unsuccessful, the process continue until a working resolution is achieved. In some cases, it can span to the next day for possible escalation and resolution.
 - No vendor must be allowed to work in the production environment without first doing same on the Test Environment
 - The remote connection must always be disconnected after each session.
 - Vendor should not be allowed to work remotely without supervision by an IT staff.

- Every unsuccessful resolution after 48 hours must be escalated immediately to IT&S.

General Remote Connection and Security Policy Rules

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.
- At no time should any company employee provide his/her login or email password to anyone, not even family members.
- Company employees and contractors with remote access privileges must ensure that their company owned or personal computer or workstation, which is remotely connected to the company's corporate network, is not connected to any other network at the same time.
- The company employees and contractors with remote access privileges to the company's corporate network must not use non company email accounts (i.e., Yahoo, Hotmail, Gmail, etc), or other external resources to conduct the company business, thereby ensuring that official business is never confused with personal business.
- All hosts that are connected to FCMB Pensions internal networks via remote access technologies must use the most up-to-date anti-virus software.
- Third party connections must comply with requirements defined by the IT & Systems Department.
- Personal equipment that is used to connect to FCMB Pensions networks must meet the requirements of the company-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the company production network must obtain prior approval from the IT Department.

General Enforcement

- Any employee found to have violated this policy shall be subject to disciplinary action, in line with the Company's staff policy
- IT & Systems Department is responsible for monitoring remote access and addressing inappropriate use of remote access privileges.

NOTE: Employee work from home request form is contained in the appendix.

Policy Code: FPL_IT_SP_10
Licence Management Policy

Policy Name: Software Acquisition & Usage & Software

Objective: Provide guidelines on appropriate use of software products utilizing company equipment

Applies to: All employees

Key guidelines:

This policy is intended to ensure that all FCMB Pensions employees understand that no computer software may be loaded onto or used on any computer owned or leased by FCMB Pensions unless the software is the property of or has been licensed by FCMB Pensions.

General

- Software purchased by FCMB Pensions or residing on company owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to FCMB Pensions' **Software Usage Policy**.
- To purchase software, users must obtain the approval of their department manager who will follow the same procedures used for acquiring other company assets.
- All approved software will be purchased through the Purchasing Department.
- Technology Solution Lead and designated members of the IT & Systems Department will be the governing body for defining appropriate software titles acceptable for use in the company.
- Under no circumstances will third party software applications be loaded onto company owned computer systems without the knowledge of and approval of the IT & Systems Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any FCMB Pensions user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
- FCMB Pensions does not condone the illegal duplication of software in any form.

Compliance

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on FCMB Pensions computing resources except as permitted in the FCMB Pensions' **Software Usage Policy**.
- Legitimate software will be provided to all users who need it. FCMB Pensions users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each user of software purchased and licensed by FCMB Pensions must acquire and use that software only in accordance with the FCMB Pensions' **Software Usage Policy** and the applicable Software License Agreement.
- Employees of FCMB Pensions are prohibited from giving FCMB Pensions acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.

Registration of Software

- Software licensed by FCMB Pensions will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software developer via procedures appropriate to that developer. Software must be registered in the name of FCMB Pensions with the job title or department name in which it is used.
- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of FCMB Pensions. A copy of the license agreement will be filed and maintained by the Legal Adviser and Company Secretary.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT & Systems Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. FCMB Pensions policy is to pay shareware authors the fee they specify for use of their products if the software will be used at FCMB Pensions. Installation and registration of shareware products will be handled the same way as for commercial software products.

Software Audit

- IT & Systems Department will conduct periodic audits of all FCMB Pensions owned PCs, including laptops, to insure the company is in compliance with all software licenses.

- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
- During these audits, the designated staff from the IT & Systems Department will search for computer viruses and eliminate any that are found.
- The full cooperation of all users is required during software audits.

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.

The ITSC will be responsible for evaluating the acquisition process.

- 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 vendor who stands out from all the rest. Other times the team may narrow the list to two or three acceptable candidates.
- If more than one vendor is selected, it can be very beneficial for the project team to talk to one or more current users of each of the potential products.
- If it can be arranged and cost-justified, an on-site visit is advised.
- The information obtained from these discussions or visits can assist in determining the vendor to be selected.

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.

Software Licence Management Policy

Currently, the Department tracks the number and type of available licenses through purchasing documentation (i.e., the PO numbers and invoices).

At the beginning of each month, the software list is reviewed to identify software up for renewal or expiring in the next three months. This list was created to maintain all software purchases for the Department and to identify renewal periods.

Software License Registration

Software must be registered in the name of FCMB Pensions Limited and the Department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The IT & Systems Department maintains a register of all FCMB Pensions software and will keep a library of software licenses. The register must contain:

- a) Application.
- b) Name of Licence.
- c) Type of Licence.
- d) Category of Licence.
- e) Unit of Licence.
- f) Date of Last Renewal.
- g) Date of Next Renewal
- h) Status.

Software on Local Area Networks or multiple machines shall only be used in accordance with the license agreement.

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

Software Licence Installation

Software must only be installed by IT & Systems Department once the registration requirements have been met. This installation right is ONLY granted to IT Staff of the Company. Once installed, the original media (If installer is not online) will be kept in a safe storage area maintained by the IT & Systems Department.

Objective: Provide guidelines on procedures and processes for Hardware acquisitions in FCMB Pensions.

Applies to: All employees

Key guidelines:

This policy is intended to establish the minimum standards for acquisition of microcomputer hardware in order to:

- a. Prevent the acquisition of technology that is defunct or out-dated while providing stable and reliable technology for operation on the company's enterprise network;
- b. Maximize the functionality of the company's information technology investment;
- c. Allow the development of open systems client/server computing that encourages connectivity, portability, scalability, and interoperability.

Policy:

All microcomputer hardware purchases must be approved by the MD/CEO or his designate. Purchases must be made by the ITSD unless a specific departure has been requested in writing with justification and such departure has been authorized in writing by the MD/CEO.

Personal Computer/LAN Workstation Minimum Hardware Requirements

- A. Must include a processor whose family and speed is comparable to current offerings of authorized computer vendors.
- B. All BIOS should be flash BIOS and upgradeable by ITSD at minimal cost to the company.
- C. RAM - All microcomputer systems must include a minimum of 1GB expandable to 2GB. 2GB is recommended.
- D. Fixed Disks - Internal disk drives with minimum capacity of 120GB must be included and supported utilizing enhanced IDE or SCSI controllers. At least one hard disk controller must be capable of controlling two (2) internal fixed disks.
- E. All microcomputers must include a CD-RW/DVD drive.
- F. Ports - All microcomputers must have a minimum of two (2) vacant high speed serial ports, one (1) parallel port, one (1) integrated mouse port and two (2) USB ports.

- G. Bays - All microcomputers must have a minimum of two (2) vacant bays. All bays must be 5.25", half-height and accessible from the front.
- H. Expansion Slots - All microcomputers must provide a minimum of three (3) vacant slots.
- I. Monitor - A minimum 15" Flat-screen monitor (minimum diagonal viewable screen size of 13.9"), non-interlaced with 0.28mm dot pitch or smaller, 1024 x 768 resolution, 256K colour, VGA display and swivel/tilt base must be included with all class configurations.
- J. Graphics -
 - 1) All microcomputers must include a minimum 32-bit graphics adapter with at least 2 MB of VRAM.
 - 2) All microcomputers offering an accelerated, 64-bit graphics adapter must include at least 4 MB of VRAM.
 - 3) Software - All workstations must be compatible with DOS and include one of the following operating systems: Windows 7, 8, 10.
- K. Clock/battery - Each microcomputer must include an internal day/date time clock with battery backup that is customer replaceable, so that date and time are maintained when the microcomputer is turned off or electrical power fails.
- L. All microcomputer systems must be capable of operating as a workstation on a network.
- M. All microcomputers must be millennium (Year 2000) compliant.

Portable Computers (Laptops and Notebooks) Minimum Hardware Requirements

- All portables must include a processor whose family and speed is comparable to current offerings of authorized computer vendors.
- All portables must have a minimum memory of 2 GB RAM. 4GB is recommended.
- All portables must include a minimum 320 GB hard drive.
- All portables must include a CD-RW/DVD drive.
- All portables must include PCMCIA support for two (2) Type II or Type I devices or one (1) Type III device.
- All portables must include one (1) parallel and one (1) high-speed serial port and at least two (2) USB ports.
- All portables must include one (1) external VGA and one (1) keyboard/mouse port.
- All portable display screens must be colour with dual scan and the screen must be a minimum of 12.1".

- All portables must include a fast charge battery with a minimum usable charge of 8 (8) hours. The battery must be of the type that remains in the unit while recharging and still allows the portable to be functional during recharge.
- All portables must include a carrying case to accommodate all hardware including the AC adapter.
- All portables must include support software for PCMCIA cards.
- All portable computers must be delivered with pre-installed operating system software unless otherwise specified. The system software must be compatible with DOS, Windows 7,8 and/or Windows 10.

Hardware Acquisition and Inventory Tracking

Purpose

- To ensure the relevance of the hardware being acquired.
- To ensure that the hardware meets business requirements.
- To ensure that the hardware is compatible with existing system.
- To ensure that the hardware is not technologically outdated.
- To ensure that the hardware can be upgraded to meet future requirements.
- To ensure that the hardware is cost effective and delivery date is in line with business requirement.
- To ensure that all hardware is properly accounted for.
- To ensure that appropriate warranty claims are made.
- To ensure that hardware disposals are approved.

Handling of User Requests

1. All users requesting for hardware and peripherals shall fill out a request form. The form must be approved by the Head of the Department.
2. The ITSD is expected to analyse the request to determine if there are alternative means of meeting the user request.
3. Where the ITSD confirms that the user's request is genuine and that there are no alternative means of meeting the user's request, they shall comment on the request form and send it directly to the ED for approval.
4. The ITSD shall document the request and follow up to ensure the request is met.
- 5 The hardware inventory shall be updated appropriately with user's requests that have been met.

Procedure for Handling Request of IT equipment

1. The requesting officer downloads the IT Request Form from the Forms Library on the intranet.
2. He submits the filled form specifying his Unit/Dept., Staff strength of the Unit/Dept., type of equipment required, quantity of equipment required, and available number of requested items in the Unit/Dept., and reason for the request to his Unit/Dept. Head for approval.
3. After due approval by the Unit/Dept. Head, the request is forwarded to ITSD who then justify/recommend for approval.
4. All ITSD recommended request shall be approved by ED.
5. All approved request must be provided from stock or procured by the ITSD in line with procurement policy.
6. The ITSD department shall handle all deployment of IT equipment.

General Guidelines for all IT Hardware Procurement

- 1) All aspiring IT Consultants/Contractors will henceforth be certified for a one-year period renewable yearly subject to satisfactory performance during the preceding period.
- 2) All prospective IT-Vendors must meet the general minimum requirements for certifications as contained in the **Vendor registration/recertification checklist**.
- 3) All prospective IT-Vendors must meet the specific requirements for the category applied for.
- 4) All certified vendors shall be given a copy of our standard/specifications based on category selected for.
- 5) All certified Vendors must submit their sealed bid when requested for, all bid not submitted within 3 days of request, shall be disqualified.
- 6) All valid bid shall be opened by the procurement officer in the presence of all members of the ITSC.
- 7) Since all certified vendors are expected to quote based on the same standard, selection of successful vendor shall be on least cost basis. Bids which fall short of standard but have the lowest price will be disqualified.
- 8) All quote documentation/bids shall be attached to a CAPEX for management approval.
- 9) Upon management approval successful vendor shall be given a letter of award.
- 10) In the event of non-performance of the preferred vendor, the reserved bidder (vendor with the second best quote) shall be called upon to supply at the bided-price of the preferred bidder. Where the second bidder cannot supply at approved price, a differential approval shall be requested from management for the agreed price.

11) All unsuccessful bids shall be communicated to the vendors within one week after the opening of bids.

Guideline on Hardware Acquisition Plan

To ensure availability of required infrastructure, ITSD is expected to prepare their acquisition plans from time to time. The acquisition plan shall form basis for raising Hardware Acquisition requests, which will be presented for top management approval. The acquisition request once approved shall be sent to ITSD for processing (see detail guideline on Hardware Acquisition)

Selection of computer hardware shall require the preparation of a specification for distribution to hardware vendors or the provision of the necessary data to enable the vendors advise on the right hardware type and configuration. This shall equally form the criteria for evaluating vendor's proposals. Consideration must be given to the under-listed points in developing the specification or in providing the necessary data required for the vendor to advise on the hardware specification:

- ❑ Organization description indicating whether the computer facilities are centralized or decentralized.
- ❑ Information processing requirement such as:
 - Major existing application systems and future application systems
 - Workloads and performance requirements.
 - Processing approaches to be used (for example, online/batch, real time databases, continuous operation)
 - Traffic Analysis
- ❑ Hardware requirement such as:
 - CPU processing speed
 - Peripheral devices (sequential devices such as tape drive, direct access devices such as magnetic disk drive, printers, CD-ROM drives, DVD-drives, WORM-drives etc.)
 - Data preparation / input devices that convert and accept data for machine processing.
 - Direct entry devices (scanners, terminals)
 - Networking capability (such as Ethernet connections, modems and ISDN connections)
- ❑ System Software requirements such as:
 - Operating System Software (current version and any upgrades required)

- Compilers
- Program library packages
- Database management packages and programs
- Communication software
- Security / access control software
- Support requirements such as:
 - Systems Maintenance
 - Training
 - Backup
 - Documentation

Adaptability requirements such as:

- Hardware/Software upgrade capabilities
- Compatibility with existing hardware/software platforms
- Changeover to other equipment capabilities
- Constraints such as:
 - Existing hardware capacity
 - Delivery dates
- Conversion requirements such as:
 - Test time for the hardware / Software
 - System conversion Facilities
 - Cost / pricing schedule

Hardware Acquisition Procedure:

1. All requests for hardware acquisitions which include PCs, Servers, Network device, Telecomm equipment, Printers and other peripherals shall be accompanied by written statement, stating the purpose or the need the hardware is to meet. It should also be stated if alternative solutions exist.
2. The Head, ITSD must ensure that the hardware or peripherals does not exist in the store before raising a procurement request.
3. A hardware specification shall be prepared which will form basis for requesting proposals from vendors. Where the exact hardware specification is not known, relevant data that will enable the vendor advise on the right hardware and specification must be provided.
4. All hardware to be acquired must be compatible with existing system. This is to avoid difficulty in integration.

5. The hardware should be up-grade-able in terms of equipment functionality and operating system requirement.
6. The hardware security and control feature must be considered.
7. The Head, ITSD shall be responsible for raising hardware and peripherals procurement requests. The request shall detail the hardware specifications.
8. The procurement request shall be directed to top Management for approval. Once the approval is given, the request shall be sent back to the ITSD for processing.
9. Testimonials/visits to other users may be necessary where the details of the performance of the system being acquired are not known.
10. There should be provision for competitive bidding. A minimum of three vendors shall be allowed to quote. Reputable organization, with track record and good financial stand shall be invited to quote. The same specification or data shall be provided to all the vendors that are invited to quote.
11. The following information shall be supplied to the vendors by the ITSD unit in the request for proposal (RFP) and the vendors are expected to quote same in their proposals:
 - ❑ Hardware configuration
 - ❑ Software Requirements (Operating System)
 - ❑ The vendors shall also be required to provide the following in their Proposals:
 - Purchase price for each if bought in single unit or in specified quantity
 - Warranty period and terms
 - Nature of support offered
 - Shipping and installation charge (if any)
 - Delivery terms (i.e. delivery date)
12. All quotations by the vendors shall be analysed against requirements.
13. The ITSC evaluate the vendors.
14. All quotations must be compared against each other and in choosing the vendors, consideration must be given to the following:
 - Vendors expertise (where it is required to facilitate the implementation)
 - Vendor pricing
 - Delivery schedule against requirement
 - Vendor financial condition
 - Vendor past performance
 - Vendors support
 - Warranty terms

- Vendor solution

15. A written report summarizing the analysis for each alternative and justification for the selected option shall be prepared and jointly signed by members of ITSC. The ITSC takes responsibility for processing the acquisition, which involves awarding the contract to the exact vendor that was chosen.

16. The letter for awarding contract shall clearly state the contract terms and the penalty for non-performance by the vendor. The following amongst others shall be stated in the letter of award:

- Hardware type and configuration
- Contract value
- Payment Terms
- Warranty and Terms
- Delivery / Completion date
- Equipment Acceptance Terms
- Penalty Clause for default

17. Copies of the letter for the award of the contract shall be distributed as follows:

- Original to the supplier
- Duplicate to ITSD
- The last copy to be retained by the ITSC.

Overview

The IT and Systems department owns computers and peripherals that no longer have value to the company. It is appropriate to dispose them by re-use, donation, auction or recycling, within the limits of this procedure.

In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of FCMB Pensions Ltd data, some of which is considered sensitive. In order to protect our data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient.

The department recognizes the importance of preserving the privacy of users and data stored in the computers. Users must honor this principle by neither seeking to obtain unauthorized access to these computers, nor permitting or assisting any others in doing the same.

Applies to: All employees

Definition

- ❑ **Used equipment** refers to any IT equipment that isn't new but is still functional. Such equipment may become available because, for example, it has been replaced by different or newer equipment.
- ❑ **End-of-Life (EoL) Equipment** refers to any IT equipment that is older than five years or too damaged, broken, or old to be functional.
- ❑ **Reuse** refers to the re-purposing (e.g., via transfer, donation, auction) of unwanted IT equipment that may still be found useful elsewhere (within the original department, or service unit or another location).

Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within FCMB Pensions Ltd including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials

Disposal Option

- ❑ **Data Removal prior to disposal:** Prior to redeployment, donation, or auction of any computer or peripheral, the data must be removed in accordance with best practice. So as to prevent unauthorized access to company's data therein.
- ❑ **Re-deploy:** Computers that are not capable of performing complex tasks may still be capable of performing simpler tasks and thus may be used either within their own or another department. Such computers must be re-deployed within the Company.
- ❑ **Donate:** Obsolete computers and peripherals that are still operational (but no longer of use to the Company) may be donated to non-profit organizations and community service).
- ❑ **Auction/Sell:** Obsolete computers and peripherals that are still operational (but no longer of use to the Company) may be sold at fair market value/auction to staffs, individuals, or for-profit entities. The auction value is recommended by the IT & System department and pass to Corporate Resources Department.
- ❑ **Recycle:** Computers and peripherals may be of such age or condition that they cannot be used for their intended purposes. These computers and peripherals should be recycled or disposed properly.
- ❑ **Warranty:** All computers and peripherals are donated or sold "as is" and with no warranties expressed or implied. Any recipient of the equipment must sign an acknowledgement of this condition.

The Policy

- **Identification:** The IT and Systems department will determine if the equipment has reached end of life or non-functional. Then compiles the list and forward it to Corporate Resources for disposal, detailing the reason(s) for such recommendations.
- **Authorization:** In all cases, the sale/auction, recycling, or donation of equipment must be approved in writing by the Executive Director of Operations & Services.
- **Local redeployment:** If the equipment is identified as suitable for redeployment (operational), the head of IT and Systems department must have approved such redeployment and a new one allocated to the previous user. When the equipment will not be recycled, the IT and Systems department is responsible for ensuring that all files have been removed from the equipment
- **Removal from Inventory:** The IT and Systems department and Corporate Resources department is responsible for removing the equipment from company's inventory lists as appropriate.

- **Employee Purchase of Disposed Items**

- Equipment which is working, but reached the end of its useful life to FCMB Pensions Ltd, will be made available for purchase by employees.
- A ballot system will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.
- Finance and Information Technology will determine an appropriate cost for each item and All purchases are final. No warranty or support will be provided with any equipment sold.
- Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to the current environmental guidelines.
- Information technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
- Prior to leaving FCMB Pensions Ltd premises, all equipment must be removed from the IT inventory list.

- **Policy Compliance**

- Compliance Measurement: The compliance/Internal Control Officer appointed will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and physical presence during such disposal.
- Exceptions: Any exception to the policy must be approved by the compliance personnel appointed or internal control in advance.
- Non-Compliance An employee found to have violated this policy may be subject to disciplinary action.

Objective: To serve as guideline towards effective innovation management

Introduction

Information Technology is seen as a driver, business enabler to achieve business goals. In order to achieve competitive advantage, business must continually strive to innovate. Effective and efficient operation can exploit and leverage information technology that results in greater business value and potentially market share. The ITSC understand innovation, recognized and encouraged it.

Key Guidelines

The goal of this policy is to:

- Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from such innovation in relation to business needs.
- Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled innovations, as well as through existing technologies and by business and IT process innovation.

Applies to: All employees

The Policy

A formal process to manage innovation allowed us to focus on current operations, and change our mindset towards the future. It provides a formal means of viewing the future of the business through a much more powerful lens – one that looks beyond the short term and encourages value creation through the qualification and staging of the most appropriate technology advances, methods and solutions.

This policy is aimed at helping the department:

1. Create an environment conducive to innovation.
2. Maintain an understanding of the enterprise environment.
3. Monitor and scan the technology environment.
4. Assess the potential of emerging technologies and innovation ideas.
5. Recommend appropriate further initiatives.
6. Monitor the implementation and use of innovation.

Processes/Tasks, Methods and Integration

- **Processes/Tasks:** The processes will involve observation and analysing of existing IT infrastructure; exploring of new technologies/solutions; reviewing the development/acquisition of new technology; analysing the direct environment (e. g. competitors' approach); analysing strategic impacts on the business and documenting of the innovation technology report.
- **Methods:** All tasks in the IT innovation management will be supported by appropriate methods. COBIT suggest methods like proof of concepts, workshops, and SWOT analyzes. In addition to strategy analysis and the use of enterprise architecture (the as-is and the to-be architecture) reviews, methods for the evaluation of innovations like checklists, value benefit analysis, net present value, compliance checks and the integration of customers into the innovation process can be used.
- **Integration:** The process is associated with defined input / output interfaces to other business strategy of FCMB Pensions Ltd. The interaction with the IT strategy development is ensured by the technology and environment (competitor) report and the monitoring of potential strategic/risk factors.

The Interaction with other Department

The IT innovation management is directly linked to FCMB Pensions Limited innovation management, as such, the intertwinement with the other departments is essential. The IT innovation management can support the "innovation decision process" by introducing new ideas for IT and Systems department. Each idea has to be evaluated for its impact and possibilities of implementation. Beyond that, IT innovation management can provide ideas for new products and services delivery during the "innovation development process". By using the IT scouting process, innovative IT systems can be found to offer new services to client (internal and external)

Roles and Responsibilities

The Head, IT and Systems Department served as the IT Innovation Manager. He represents the innovation management both inside and outside the company. He is also responsible to liaise with other industry player for identifying new ideas and trends and implement same within the company.

All employees are also encouraged to report and discuss ideas with the innovation manager. These ideas have to be sorted and categorized by the IT innovation manager. They need to be evaluated

and prioritized. To explore these ideas, the IT innovation manager upon approval from ITSC can start pilot projects to evaluate such innovation.

If a discovered IT innovation proves to be strategically important for the company, the IT innovation manager has the competence to escalate ongoing IT projects that run contrary to this innovation to ITSC.

After an innovative idea has been established, the Business Development, Operation Department and ITSD needs to evaluate such idea in the overall interest of the company. After defining the innovation systems' scope and identifying relevant actors, the ITSC will analyze the organization's environment and filter relevant information for the innovation processes in the organization. Therefore, appropriate information channels (like newsletters, analyst reports and websites of competitors, benchmarks, etc.) have to be identified. The information gained will be evaluated and filtered. A proactive report will then be presented which summarize specific trends or activities of competitors or the industry at large.

The innovation report is a helpful instrument for developing and revising our IT strategy document. In addition to that, a systematic definition of the innovation systems provides orientation for strategic alignment. The implementation of new IT innovations can contribute to the generation of new business models and new business strategies. A pilot projects can be used to explore and evaluate the new innovation and technologies with an emphasis on risk and potentials.

Objective: To keep the components that form part of information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

Introduction

Patch management is an important part of keeping the components of the information technology infrastructure available and usable to the end user. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

Scope

- i. This policy applies to all components of the information technology infrastructure deployed within the Company:
 - a. Computers
 - b. Servers
 - c. Application Software
 - d. Routers and switches
 - e. Databases
 - f. Storage
- ii. All staff within the IT & Systems Department must understand and use this policy. IT staff are responsible for ensuring that the vulnerabilities within the IT infrastructure are minimized and that the infrastructure is kept patched up to date.
- iii. All users have a role to play by ensuring that they allow patches to be deployed to their workstation.

The Policy

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security or update patches. System components and devices attached to the company's network shall be regularly maintained by applying critical security/update patches after review and approval by the Head of the Department. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as at when due. Application patches shall also be review, deployed on a test environment and certified suitable before deploying to production environment.

System, Utility and Application Patching

- i. The organization's anti-virus server will be configured to automatically download the latest virus and spyware definitions.
- ii. Notifications of patches from application and database vendors will be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the suppliers website will be reviewed on a regular basis.
- iii. The websites of the suppliers of servers, storage, PC's, tablets, printers, switches, routers and peripherals will be reviewed to determine the availability of firmware patches as approved by the HOD.
- iv. Missing patches identified will be implemented appropriately as approved.
- v. Web based application patches shall upon certification and approval by the HOD be deployed on the server and propagate to every nodes accessing it while Windows based application shall upon certification and approval by the HOD deployed on the server and if needed deployed across every workstation that required it. The regular application of critical security patches will be reviewed as part of normal change management procedures.

Type of Patches

Type	Patches	Mode
Server/ Computer	Drivers/ firmware	Automatic/Manual
Operating system	Service packs	Automatic/Manual
Application software	Service packs, feature packs	Manual
Routers and Switches	Firmware	Automatic/Manual
Printers and Scanners	Drivers, firmware	Automatic/Manual
Anti-virus/ Anti spyware	Data file/ Virus definition update.	Automatic/Manual

Patching Exceptions

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. A test server is the most preferred destination of all patches received from vendor to avoid disrupting the service delivery. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require HOD's authorization.

Security Patching Procedures

The process shall ensure that application, system, and network device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable to vendor-supplied tools on a regularly communicated schedule
- Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

Audit Controls and Management

On-demand documented procedures and evidence of test should be in place for this operational policy as part of IT & Systems Department change management procedures. Examples of adequate controls include:

- Documented change request/meetings and conversations between key stakeholders
- Application/Vendor based updates and patch must be documented for all service applications (This should include version, date patched, patch status, purpose, exception, and reason for exception, and approval)
- All patches must be downloaded from the relevant system vendor or other trusted sources. Each patch's source must be authenticated and the integrity of the patch verified.
- All patches must be submitted to an anti-virus scan upon download.
- All patches must be tested prior to full implementation since patches may have unforeseen side effects.
- New servers and desktops must be patched to the current agreed baseline before deployment to production environment.
- A back out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in the event that the patch has unforeseen effects.

Ownership and Enforcement

- i. The IT Department will be responsible for identifying patches for the application systems which they administer.
- ii. IT Department will use restore points where practical to ensure rollback changes.

- iii. The HOD will be responsible for patch approval and ownership of all technical updates including: operating systems, patches for workstations and servers, antivirus and antispyware, drivers of devices
- iv. Staff members found in policy violation may be subject to disciplinary action as maybe determine by the Management.

1. Purpose

This procedure provides a framework for the IT & Systems Department to evaluate and improve the performance of all Suppliers and Vendors that are sourced by the department or the Company for IT service delivery, to:

- i. Pro-actively managing the performance of Vendors during the term of awarded contracts; and
- ii. Creating a record of past performance for use by the company, in determining the award for future solicitations and contracts.

IT & Systems department may utilize this document for all contracts including but not limited to; invitational bids, single or sole source purchases, emergency purchases and wherever it is in the best interest of the company.

2. Vendors' SLA Management (Applicable to ALL Critical Vendors)

Every vendor providing core service are expected to have a signed and approve SLA properly vetted by the Legal department.

Key content of the SLA includes among others the following:

- Contract duration
- Start and end dates
- Description of the contract
- Responsible contact person on Legacy Pension side with contact details
- Designated Business Relationship Manager on the vendor's side with contact details
- Statement of acceptable usage
- Termination statement
- Statement of Confidentiality
- Fault and fault resolution procedure
- Facilities, Infrastructure and Licensing
- Service Support and maintenance
- Indemnity, Reliability and availability statement
- Warranty statement
- Conflict resolution
- Notices and variation
- Financial obligation
- Force majeure
- Waivers and amendment

3. Vendor Performance Evaluation Form

The vendor performance evaluation form is to be used periodically to evaluate compliance of each vendor in meeting quality service delivery as contain in the contract agreement/SLA.

3.1 Frequency of Performance Evaluations

Product/service shall be evaluated at least once every twelve (12) months for all contracts with a term longer than one (1) year. Additional performance evaluation forms may be completed and discussed with the vendor at any time throughout the term of the contract as needed, based on the Vendor's performance.

3.2 Product/Service users and/or IT & Systems Department should complete a **Performance Evaluation Form** for all products/service in use, in a timely manner of the following occurrences, depending on the type of products or services:

- For Consulting contracts; upon completion of the Contract;
- For Products/equipment; upon delivery and inspection of the products;
- For Software, upon completion of implementation or during usage
- Upon termination of a Contract for any reason prior to the Contract end date.

3.3 Vendor's receiving a Performance Evaluation Form with a rating of **CAUTIONARY OR BELOW**, in any category, should be requested in writing, to provide, a written response and appropriate corrective action within an acceptable timeframe, in accordance with the Terms and Conditions of the solicitation, or at the discretion of the Company. Failure of the Vendor to do so, in the sole opinion of the Company, may lead to termination of the Contract.

4.0 Recommended Steps to Resolving Vendor Performance

4.1 It is important to have open communication with the Vendor throughout the Product/Service life and to inform the Vendor in writing when their performance is a concern and to request appropriate corrective action within an acceptable timeframe, in accordance with the Service Level Agreement. It is equally important to keep a written record of all correspondence with the Vendor.

4.2 If the Vendor's response or corrective action is still a concern, the departmental can request the IT Steering Committee to recommend appropriate action on the said vendor.

5. Record Retention

IT and Systems department shall maintain the following documents, following the completion of the Product/Service deployment or maintenance period as supporting rationale to augment the Performance Evaluation Form:

- i. Internal and external correspondence (e.g. Emails, letters, chat etc.);
- ii. meeting resolution (on-site or off-site) describing all issues discussed, decisions made, issues unresolved, and action taken;
- iii. progress reports;
- iv. Product/Service diaries which record significant issues of concern;
- v. Rejected Product/Service deliverables;
- vi. Any other type of correspondence or record not listed above.

6. Performance Evaluation System

6.1 During evaluation, each vendor shall be assigned one of the following ratings to each category set out on the Performance Evaluation Form. A critical aspect of the assessment rating system described below is the **second sentence** of each rating that recognizes the Vendor's resourcefulness in overcoming challenges that arise in the context of product/service performance.

Rating		Description of Rating
9 - 10	Exceptional	Performance significantly exceeds Contract requirements to the Company's benefit, for example, the Vendor implemented innovative or business process reengineering techniques, which resulted in added value to the company. The contractual performance of the element or sub-element being assessed was accomplished with few minor problems for which corrective actions taken by the Vendor were highly effective.
7-8	Good	Performance meets contractual requirements and exceeds in some area(s) to the Company's benefit. The contractual performance of the element or sub-element being assessed was accomplished with some minor problems for which corrective actions taken by the Vendor were Effective.
5-6	Satisfactory	Performance meets contractual requirements. The contractual performance of the element or sub-element contains some minor problems for which proposed corrective actions taken by the Vendor Appear satisfactory, or completed corrective actions were satisfactory.

3-4	Cautionary	Performance did not quite meet contractual requirements. The contractual performance of the element or sub-element contains some minor problems for which proposed corrective actions taken by the Vendor appear to be a continued minor concern, or completed corrective actions were slightly below satisfactory.
0-2	Unsatisfactory	Performance does not meet some contractual requirements. The contractual performance of the element or sub-element being assessed reflects a serious problem for which the Vendor has submitted minimal corrective actions, if any. The Vendor's proposed actions appear only marginally effective or were not fully implemented.

6.2 Final Performance Evaluation report shall be used by the department for future consideration of award, to determine if a vendor submitting a bid is a responsible vendor or not.

A Vendor that has received a **TOTAL** rating of **27-50** on the Final Performance Evaluation Form:

- a) will be considered a Responsible vendor for future similar proposal submissions to the Company,
- b) For a multi-year term Contract, the Contract may be extended for up to additional two (2) one (1) year terms, at the discretion of both the Company and the Vendor. Price adjustments for the extension shall be based on one of the following:
 - i. any inflationary contract annual increase either stated in the original solicitation document or stated by the Vendor in their original bid submission; or
 - ii. The same costs as stated in a firm fixed price multi-year Contract.

Where a solicitation document did not state or request any inflationary annual Contract increase or where the Vendor is not agreeable to continuing the contract at their prices within a firm fixed price multi-year Contract, the contract extension will not apply and the IT Steering Committee may request a public solicitation to receive new bids.

6.4 A Vendor that has received a **TOTAL** rating of **(15-26)** on the Final Performance Evaluation Form;

- a) may or may not be considered a Responsible Bidder for future similar Bid submissions to the
- b) Company; and
- c) For multi-year Contracts, is not eligible for any extension terms within the current Contract.
- d) may be asked to demonstrate in writing or by other acceptable means to the Risk Manager/Auditor, that they have corrected all previously documented areas of **"CAUTIONARY" OR LESS** performance concerns to a standard satisfactory to the

Company, prior to awarding any future Contracts. In addition, a list of new references may be requested by the Company for work completed by the Vendor since the date of the Performance Evaluation Form where a rating of **"CAUTIONARY" OR LESS** was given in any category. The Company reserves the right, at its sole discretion not to award a Contract to any Vendor, for an indefinite period that fails to provide satisfactory evidence of correcting any documented past performance concerns by the Company.

6.5 A Vendor that has received a **TOTAL** rating of **less than 15** on the Final Performance Evaluation Form;

- a) shall not be considered a Responsible Bidder and shall be disqualified (barred) for a minimum two
- b) (2) year period, to a maximum of five (5) years, at the discretion of the Company; and
- c) for a multi-year Contract, is not eligible for an extension term to the current Contract; and
- d) may have their current Contract with the Company terminated at any time, due to poor performance; and
- e) Will receive a letter issued by the Company, confirming the Disqualification Period and setting out the requirements for reinstatement.

6.6 Any vendors that refuses or fails to execute a Contract awarded to her by the Company may be subject to a Disqualification Period, at the sole discretion of the Company.

6.7 Where a Contract has multiple departments or agencies completing an Evaluation, the Vendor's overall performance rating for either an Interim Evaluation or Final Evaluation shall be based on the lowest evaluation rating received by a department or facility.

7.0. Vendor Response and Appeal Process

The Vendor shall have ten (10) business days to:

- a) Submit a written response to the Final Performance Evaluation, using the Company's response form and /or
- b) Submit a written request to appeal a Final Performance Evaluation rating, utilizing the Company's response form.
- c) If no response is received within the above noted timeframe the Evaluation rating shall be considered final.

7.1. APPEAL PROCESS

Within ten (10) business days) of receiving an appeal response form in respect to a Final Performance Evaluation Form, the Company will conduct a full review of the appeal and render a final decision based on

the appeal information. The Company may request additional information from the Vendor in order to conduct a full review. Any Disqualification Period in place, shall be upheld during an appeal under review by the Company. The Company's decision shall be final and binding on all parties.

Introduction

Cloud computing services are typically provided by third parties using Internet technologies. There are four widely accepted service delivery models:

- Infrastructure as a Service (IaaS);
- Software as a Service (SaaS);
- Platform as a Service (PaaS);
- Network as a Service (NaaS).

Cloud services can be provided via four deployment models:

- Private cloud – where services are provided by an internal provider;
- Public cloud – where services are provided by third parties, i.e. external companies or entities, over the public Internet;
- Community cloud – where services are provided by external company(s) or entity(s) for a specific community of users with common interests;
- Hybrid cloud – where services are provided partly by an internal provider in a private cloud and partly provided by an external company(s) or entity(s) in the public or community cloud.

Purpose: This policy provides a governing framework for all infrastructure deployed by FCMB Pensions Limited in the cloud. It applies to all personal data, sensitive personal data and confidential business data and information (to include legal documents not already in the public domain). It covers SaaS, IaaS, PaaS, NaaS etc.

THE POLICY

All staff and organisations acting for, or on behalf of, the company in the procurement or evaluation of cloud services, or planning on using cloud services to store or process data or information obtained through their interaction with the company must ensure that the following steps are adhered to:

- Use of cloud computing services for work purposes must be formally authorized by the ITSC upon clarification and certification by the Head, IT that security, privacy and all other IT best practices requirements has been adequately addressed by the cloud computing vendor.

- Approval that data or information can be hosted in the cloud: Following approval from ITSC. Where a cloud service is proposed to host personal data, personal sensitive data or confidential business data and information, then before entering into a cloud service agreement the proposed cloud service must be reviewed, tested as appropriate, and approved to ensure that confidential data can be processed and stored securely.
- The Company places great emphasis on the need for integration (all systems should be able to talk to each other) and interoperability (systems should be able to work on and be moved to different environments) of systems. These requirements must be considered and documented.
- The use of cloud services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by FCMB Pensions.
- All Cloud Services must be fit for the purpose they are designed to support; and comply with all relevant legislation and compliance in the Country.
- Cloud Backup and Retention: The cloud service provider must be able to ensure that the data and information is secure at all times and that an adequate backup and recovery plan is in place to ensure that data and information can be retrieve in a timely manner to meet business ness. For more critical systems, the service must be built with high availability, with a business continuity and disaster recovery plan that fits business needs.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.
- We must respect the intellectual property rights of clients and not breach copyright when using cloud services.
- Employees must not share their log-in credentials with co-workers.

RISK ASSESSMENT

The following non-exhaustive list of issues should be taken into account before considering any cloud computing solutions for FCMB Pensions:

- The IT priority needs of the Company and the related business case;
- The type of information and data to be stored, their confidentiality and sensitivity (e.g. e-mails, archival records, correspondence with third parties, financial information, meeting records, etc.);
- the country where the service provider or the cloud servers is located;
- the type of cloud solutions and configurations available and their cost and efficiency;
- the available risk mitigation measures and mitigation costs for external, public and hybrid clouds, including through encryption of data, segregation of data, and appropriate contractual clauses;
- Whether storage of the information and data in question requires the agreement of, or at least consultation with, staff and/or third parties.

ROLES AND RESPONSIBILITIES

All engaged by the company are responsible to:

- Consider security and privacy requirements when evaluating and selecting potential vendors for services;
- Ensure that a formal agreement has been reviewed by the Legal department prior to the signing and acceptance of the agreement;
- Ensure the Legal department receives a current copy of a third parties Attestation of Compliance or Report on Compliance with Nigeria Data Protection Act.
- Ensure that the confidentiality of sensitive and personal information is protected by only using approved features and functionality from approved cloud computing service providers;

VENDOR'S PERSONAL IDENTIFICATION INVENTORY (Please see Appendix)

Policy: All software products developed by/for the company must be designed to meet agreed standard set by IT & Systems department.

Purpose: To standardize software development for all enterprise-level centrally-managed mission critical applications and services created.

Scope: Applies to all employees, consultants involved in the development or modification of enterprise-level, and centrally-managed mission critical applications. All software products and updates released by/for the company.

Policy Statement:

- If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.
- All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this Policy addresses the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design specification; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This ensures that the software will be adequately documented and tested before it is used for sensitive information.
- These standards include: coding techniques, testing strategies, documentation requirements and software release processes that align with industry standards and regulatory requirements. There must be a separation between the production, development and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions.
- All development work shall exhibit a separation between production, development, and test environments, and at a minimum have at least a defined separation between the development/test and production environments unless prohibited by licensing restrictions or an exception is made. These separation distinctions allow better management and security for the production systems, while allowing greater flexibility in the pre-production environments.
- All application/program access paths utilized in development or testing, other than the formal user access paths, must be deleted or disabled before software is moved into production.

- Documentation must be kept and updated during all phases of development from the initiation phase through implementation and ongoing maintenance phases. Additionally, security considerations should be noted and addressed through all phases.

Exclusions or Special Circumstances:

Exceptions to this policy and associated standards shall be allowed only if previously approved and evidence of such approval documented and verified.

The Policy - GENERAL

Regardless of the software development methodology used (waterfall or agile), all methodologies have similar activities associated with successful execution. The Application Developer shall be responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC) for FCMB Pensions. All software developed in-house which runs on production systems shall be developed according to the established processes and procedures of the SDLC. At a minimum, SDLC activities and tasks should address the following ten activity areas:

1. Project Initiation/Definition
2. Risk Assessment
3. User Requirements (Functional and Non-functional)
4. Technical and Architectural Systems Design
5. System Programming or Customized Off the Shelf (COTS) Software Development /Acquisition
6. Quality Assurance
7. Documentation and Training
8. Systems Testing and User Acceptance testing
9. Installation/Deployment
10. Maintenance

The Developer shall have the flexibility to determine the means and details of methodology implementation with the provision that whatever development and delivery mechanism chosen addresses each of the major project elements listed above, is consistent, and is applied across the life cycle.

- Role Based Access Controls

All Custom off the Shelf ("COTS") and custom application production systems must have a role-based access control system to restrict system access privileges to users. Systems shall have designated access control administrators who manage system wide privileges for user roles. Should the access

control administrator also be a regular user of the system, they shall have two role-based accounts – one for administrative access and one for user-based access.

- Three Tier Development Environment

There shall be a separation between non-production and production application environments to reduce the risks of unauthorized access or changes and aid in supporting methodology execution.

The three operational environments are as follows:

Development – The development environment is predominantly accessed by application programmers creating and testing new functionality, functional enhancements, and bug fixes. Developers have full control over this environment and it is not considered to be a “stable” code platform as active development is occurring within the logical instance. Once enhancements have been unit tested and certified for quality assurance, they should be moved in a stable testing environment. The following policy and procedure apply to the development environment:

- Development systems must not contain sensitive or confidential information and shall be populated with test or dummy data
- Access to program source code shall be restricted to authorized personnel and managed using versioning tool like Git.
- All internally developed must:
 - Adhere to company’s coding standard
 - Implement OOP using design paradigm
 - Conform to SOLID design principles
 - Comply with software design patterns

Test – This environment more closely mimics the production environment. Quality assurance and user acceptance test personnel operate in this environment to test enhancements and bug fixes scheduled for release into production. The environment is continually refreshed with test data and new functionality until such point the release is deemed stable and ready for promotion into production.

The following policy and procedure apply to the test environment prior to applications being promoted to production:

- Application-program-based access paths other than the production access paths must be deleted or disabled
- Software debugging code must be removed
- Test User IDs and passwords must be removed

- All pre-production code shall be reviewed and certified prior to release to identify any potential coding vulnerability. The following procedures shall be followed:
 - Code changes shall be reviewed by individuals other than the originating code author and by individuals knowledgeable about code-review techniques and secure coding practices
 - Results of testing are reviewed and approved by the HOD prior to release
 - The requirement for code reviews applies to all custom code (both internal and public facing), as part of the change management promotion process
 - Code reviews and use-case tests shall be conducted by knowledgeable internal personnel or third parties
 - Public facing web applications are also subject to additional controls to address on-going threats and vulnerabilities after implementation
 - Development team will move programs from development into production on a structured release schedule communicated to users and approved by the HOD.
 - Software developers shall not be permitted to move programs into the production environment directly unless expressly authorized by the HOD.

Production – This is the operational environment for the current release of the application. The production environment is subject to stringent change management processes and procedures to limit risk and functional downtime to systems.

This system architecture and infrastructure ensures that security and stability is rigorously maintained for the production system while development and test environments maximize software development productivity.

Program Data Owners

All production systems must have designated Program Owners/Custodian for the critical information they process and act on. Program owners ultimately control the release of new software into production based on testing results. The following applies to Program/ Data Owners:

- Acceptance signoff is required to promote pre-release test code into production
- Test results shall be reviewed and provide prior approval prior to moving new software or software updates into production
- Data owners shall also review and approve data migrations or system integrations from one application system to another

Quality Assurance and Production Delivery

Managing the quality of the delivery methodology is key to the success of application development execution. The following procedures shall be implemented related to software delivery:

- The development of all software shall be supervised and monitored by the HOD and shall include security requirements, periodic independent security review of the environment, certified security training for software developers, and ad-hoc code reviews
- Applications shall be securely designed, coded, and maintained in accordance with industry accepted security standards and comply with applicable statutory, regulatory, legal and business requirements
- Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data
- Quality assurance procedures shall include systematic monitoring and evaluation of software developed, outsourced, or acquired by the Company.
- Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established and documented.
- Tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security
- Test data shall be carefully selected, protected, and controlled
- Management shall have a clear oversight capacity in the quality testing process with the final product being certified as fit for its desired purpose
- Procedures shall control the risks related to production software and hardware changes that may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications. This includes the following:
 - Separate three-tiered operational environments shall exist with enforced accesses controls
 - Discrete separation of responsibilities shall exist between development, test, and production environments
 - Production data shall not be used for testing or development purposes
 - Processes shall exist for the removal of test data and accounts before production systems become active (where appropriate)
 - Change control procedures shall exist for security patches and software modifications including:

- Change Impact Documentation
- Authorized Change Approvals
- Pre-Release functional testing to verify that the change does not adversely impact system security
- Roll-back procedures

Software Development Version Management

Once developers have the appropriate sandbox for the development phase of code, the next step is giving them a place to control and track changes. Version control systems take a repository of your code and project files and keep a history of all changes, which makes it easy to edit the code - while still understanding it - in the long run. The company uses Git for code repository and version control system.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the internal application development and release methodology. Examples of appropriate controls and management include:

- Evidence of software development methodology process artifacts across multiple project implementations
- Demonstrated change management processes and procedures
- Evidence of physical three-tier delivery environments
- Historical evidence of sustained practice (email, logs, interviews)

Requirements for Secure Software Development Practice

All software must benefit from its developer's adherence to secure software development practices. Software does not exist in a vacuum (e.g., it is often collocated with other applications); a weakness in one application can become an attack vector to gain access to other applications or data. IT Application developers must follow secure software development practices during the entire software development lifecycle and implement controls appropriately. The layering of security controls helps prevent or detect breach attempts and can reduce the time required to detect and respond to attackers. Applications need to be secure so they are not exploited to attack users with malware downloads or redirects to malicious sites.

Input Validation:

IT Developer team must:

- Validate user input before using the input data programmatically.
- Sanitize or reject invalid user input to protect against code injection attacks.
- Include user interface controls in the input validation strategy to make compliant and safe input easy for the user.
- Protect against buffer overflow attacks.
- Protect against array index errors.
- Protect against parameter manipulation attacks.
- Use parameterized SQL queries.
- Defend against SQL injection attacks.
- Put all SQL code/commands in server-side code.
- Set Autocomplete=off in HTML to prevent the caching of sensitive information.
- Protect against URL query string manipulation attacks.

Exception and Error Handling:

IT Developer team must:

- Configure runtime environments so that they do not reveal native framework errors (e.g., .Net, J2EE) to the screen/browser.
- Set up custom error pages for framework errors.
- Handle expected errors and provide users/administrative staff enough detail in error messages to troubleshoot problems.
- Write code so there are no unhandled errors.
- Create (wrap code) last-resort error try-catch blocks and never use empty catch blocks.
- Ensure catch blocks cause the application to stop running and exit in a secure state.
- Log detailed exception and error messages to the application event logs

Cross Site Scripting (XSS) and Invalidated Redirects/Forwards:

IT Developer team must test untrusted data or code before sending it to a web browser. Testing must include proper validation for common XSS attacks.

Insecure Direct Object References:

IT Developer team must ensure that direct object references to any object, file, directory or database key include an access control check or other protection.

Transport Layer Security (TLS) and Secure APIs:

IT Developer team must:

- Force HTTPS for all browser connections and Disable HTTP.
- Use TLS 1.2 or later to protect machine-to-machine connections (e.g., app server to DB server connections).
- Use strict transport security header and adhere to agreed encryption technology.
- Encrypt APIs, restful interfaces, extract tools and service bus sessions.
- Authenticate APIs, restful interfaces, extract tools and service bus sessions.
- Never store user passphrases and never hardcode credentials
- Protect service account credentials with established tools and techniques.
- Implement session timeout and lockout after 5 failed authentication attempts.
- Delete, remove and invalidate tokens (when used) on logout.
- Prominently display the logout function throughout the application.

Secure Configuration

IT Developer team must:

- Use secure configuration options for supporting technology, libraries, packages and tools.
- Perform or have performed a vulnerability scan of the entire solution and appropriately remediate findings based on risk before placing the solution into production.
- Secure the components used in an application.
- Run components with the least privilege possible and keep components patched and up-to-date.
- Execute SQL with the least privilege possible.
- Use vetted and tested hardening guides to ensure the correct application of options and settings.
- Define, implement and maintain secure settings (e.g., do not rely on default settings).
- Secure the software configuration used in an application.
- Set the configuration to define which HTTPS methods (e.g., Get or Post) the application will support and whether HTTPS methods will be handled differently in different pages of the application.

Software Development Standards/Guidelines

The purpose of these set of standards is to improve the readability of a software and focuses on good internal documentation practices for the IT software developer of FCMB Pensions. Regardless of the programming language used to write any piece of software.

Indentation

Proper and consistent indentation is important in producing easy to read and maintainable programs. A minimum of 4 spaces shall be used to indent. For convenience, a single tap on the Tab key is fine.

Examples:

```
// indentation used in a loop construct
for (int i = 0; i < count; i++) {
    total += i;
}

// indentation used in the body of a method
function printHello() {
    console.log('Hello World!');
}
```

Use of Braces

Programmers shall use either of the following bracing style:

```
function functionName()
{
    // do something
}

or

function functionName()
{
    // do something
}
```

Classes and Functions

Classes names should be well represented and contain only properties and methods related to the class. Single Responsibility Principle (SRP) should be adopted, instead of trying to do too many activities within a single class.

Keep functions/methods reasonably sized. If a method does a lot of task, break it down into subtasks which can be handled by new routines or methods.

Spacing

The proper use of spaces within a line of code can enhance readability. Good rules of thumbs are as follows:

- A keyword followed by a parenthesis should be separated by a space
- A blank space should appear after each comma in an argument

Example

```
cost=price+(price*salesTax); // not accepted
cost = price + (price * salesTax); // accepted
```

Variable/Function Names

Variables/functions shall have meaningful names that convey to a casual observer, the intent of its use. Shortening variable/function name is not allowed.

```
// variables
var totalSalary = 3000; // accepted

var ts = 3000; // not accepted

var totalSal = 3000; // not accepted

// functions
function calculateTotalSalary(basicSalary, housingAllowance, ...) { // accepted
    // computation logic goes here
}

function calcTotalSal(basic, housing, ...) { // not accepted
    // computation logic goes here
}
```

Comments

Comment your code where necessary to explain or give a brief of what is happening in your code.

Inline comments promote program readability. They allow a person not familiar with the code to more quickly understand it. It also helps the programmer who wrote the code to remember details forgotten over time. Writing a well-structured program lends much to its readability even without inline comments.

Classes, functions/methods should be also be documented where necessary for the reasons stated above.

Meaningful Error Messages

Error handling is an important aspect of programming. Try as much as possible to write codes that will not crash while in use. Error messages should be meaningful. When possible, they should indicate what the problem is, where the problem occurred, and when the problem occurred. Error messages should be logged to a file or send as an email to the developer. Code which attempts to acquire

system resources such as dynamic memory or files or object that could return null should always be tested for failure.

```
var employee = dataContext.Employees.FirstOrDefault(e => e.ID == staffId);  
if (employee != null {  
    // proceed  
} else {  
    throw new Exception($"There was no employee found with the ID: {staffId}");  
}
```

Policy Code: FPL_IT_SP_18

Policy Name: Backup & Recovery Policy

Purpose: The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. This document is intended to provide details on the stipulations of data backup and retrieval operations to the client.

Scope: The intended recipients of this policy are members of the ICT Department and disaster recovery team.

Policy: Information Technology recognizes that the backup/ recovery and maintenance of data for servers are critical to the viability and operations of the respective departments in the organization. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis and recovery of electronic information in the event of failure.

Backup Content: The content of data backed up varies from server-to-server. The primary data that will be backed up are: Data files designated by the respective owners of the servers and in some instances System Data (Applications files for the server and other selected software installed on the server). Data to be backed up will be listed by location and specified data sources. This will be stipulated in a separate document called "Data Sources Manifest". Because it is impractical for the Systems Support to back up every bit of data stored on the servers, the only data that Systems accepts responsibility for is the data which is explicitly listed in the "Data Source Manifest"

Recovery Content: the recovery content is "same as is" what is backed up in the backup content. This is so because failures can take many forms, and may occur over time, multiple generations of backups should be maintained and recovery test conducted periodically.

Policy Code: FPL_IT_SP_19

Policy Name: Database Management Policy

1.0 Objective: To establish uniform data management standards and identify the shared responsibilities for assuring the integrity and efficiency of the company's data.

1.1 Applies to: All employees whose job responsibilities include inputting, safeguarding, retrieving, or using data, and to those who supervise such individuals.

1.2 Purpose:

The purpose of this policy is to establish a framework of principles to be applied to the management, security and use of corporate data within FCMB Pensions Limited.

Definition:

- **Enterprise Master Data** means data from a primary source
- **Primary Source** means the official Company record for the relevant data, as identified by the data owner, i.e. where data is 'mastered'
- **Restricted Data** means data that is protected by legislation or policy and that requires the highest level of access control and storage protection
- **Secondary Source** means a source of data that has been copied from a primary source.
- **Data quality** – the accuracy, completeness, validity and currency of data

1.3 Principles of Data Management

The following principles of data management outline best practices at a high level within FCMB Pensions. Every Data Custodian must be aware of these, and adhere to them. This ensures contributions to data quality are being made at all levels within the company.

These principles must guide all data management procedures.

- The Company, rather than any individual or business unit, owns all data.
- Every data source must have a defined Custodian in a business leadership role, who
 - b. Has overall responsibility for the accuracy, integrity, and security of those data.
 - Wherever possible, data must be simple to enter, be clearly defined and accurately
 - c. Document their subject. They must also be in a useful, usable form for both input and output.
 - Data should only be collected for a specific and documented purpose.

- Data must be readily available to those with a legitimate business need.
 - Data capture, validation, and processing should be automated wherever possible.
 - Data must be entered only once.
 - Processes that update a given data element must be standard across the information system.
 - Data must be recorded as accurately and completely as possible, by the most informed source, as close as possible to their point of creation, and in an electronic form at the earliest opportunity.
- d. Data should be recorded and managed over time in an auditable and traceable manner.
 - e. The cost of data collection must be minimised.
 - f. Data must be protected from unauthorised access and modification.
 - g. Data must not be duplicated unless duplication is absolutely essential and has the approval of the relevant Data Steward. In such cases, one source must be clearly identified as the master; there must be a robust process to keep the copies in step; and copies must not be modified (i.e., ensuring that the data in the source system is the same as that in other databases).
 - h. Data structures must be under strict change control, so that the various business and system implications of any change can be properly managed.
 - i. Whenever possible, international, national, or industry standards for common data models must be adopted. When this is not possible, organisational standards must be developed, documented and implemented.
 - j. Data should be defined consistently across the Company.
 - k. Users must accurately present the data in any use that is made of them.
 - l. Schemas that describe the data must be developed and maintained for as long as they describe are in use, and these must be maintained separately to the systems that manage the data.

2.0 Data Administration

2.1. Ownership of Administrative Data

All Administrative Data is owned by FCMB Pensions. As such, all members of the company have the obligation to appropriately use and safeguard the asset, in all formats and in all locations.

2.2 Data Classification

Administrative Data is categorized as High Risk, Confidential Risk, and Public following the Data and Information Security Policy and should be safeguarded appropriately. It is essential that all FCMB Pensions data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.

FCMB Pensions classifies data in the following three classes:

High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.

- Data covered by the Pension Reform Act are in this class.
- Payroll, personnel, and financial information are also in this class because of privacy requirements.
- FCMB Pensions recognizes that other data may need to be treated as high risk because it would cause severe damage to the company if disclosed or modified.
- The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential – Data that would not expose the company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public - Information that may be freely disseminated.

- All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through FCMB Pensions.
 - Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level.
 - No company owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
 - Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
 - High risk and confidential data must be encrypted during transmission over insecure channels.
 - All appropriate data should be backed up, and the backups tested periodically.

- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

2.3. Access and Confidentiality

Access to the Company Data should be based on the business needs of the organization and should enhance the ability of the Company to achieve its mission. Employees shall have access to the Administrative Data needed to perform their responsibilities. Individually identifiable data shall be available to the extent necessary to perform administrative tasks.

In order that the proper controls are applied, it is the responsibility of each person accessing Administrative Data to:

- a. Know the classification of the system being used.
- b. Know the type of Administrative Data being used.
- c. Follow the appropriate security measures.

2.4. Training

Before an individual is permitted access to Administrative Data in any form, training in the use and attributes of the data, functional area data policies, and Company policies regarding data is strongly encouraged.

2.5. Integrity, Validation, and Correction

Administrative Data must be safeguarded and managed in all formats and media (e.g., print and digital), at all points of access, and across all Company systems through coordinated efforts and shared responsibilities.

2.6. Extraction, Manipulation, and Reporting

Extraction, manipulation, and reporting of Administrative Data must be done only for Company business purposes, or subject to terms of use as otherwise approved by the IT Steering Committee. Personal use of Administrative Data, in any format and at any location, is prohibited. All data users are expected to be familiar with and conform to the Company's Data management policy.

3.0 Data Management Roles and Responsibilities

3.1. IT Steering Committee

IT Steering committee are responsible for planning and policy-making for Administrative Data and for the establishment of operational processes to collect and record data in accordance with the Company business rules.

3.2. Data Steward

Data Stewards are typically operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the Transactional Systems.

3.3. Data User

Data Users are individuals who access Administrative Data to perform their assigned duties. Data Users are responsible for safeguarding their access privileges, for the use of the Administrative Data in conformity with all applicable policies, and for securing such data.

3.4. Data Custodian

The Data Custodians are IT staff assigned to each transactional and reporting system which maintains Administrative Data. Data Custodians oversee the safe transport and storage of data, establish and maintain the underlying infrastructure, and perform activities required to keep the data intact and available to users.

- **Database Standards:** All databases must be set up and configured in conformance to the company operating processes.
- **Access Privileges:** Access privileges must be closely monitored and in accordance with policies and standards defined in the Details Information Security Policy. Formal administration process that requires manager-level authorization for all users to the database, and supporting utilities must be defined. (See User Access Control contained in the Standard and Procedure Document).
- Sensitive database utilities will be restricted to personnel responsible for the maintenance of the databases.
- Within the production system, Change Requests (CRs) are required to alter data outside of the transactional schedule and must adhere to the policies contained under Change Management Policy.

1.0 Objective: To achieve standardization on our information gathering, usage, dissemination of such data and its protection.

1.1 Applies to: All employees whose job responsibilities include inputting, safeguarding, retrieving, or using data, and to those who supervise such individuals.

1.2 Purpose:

The purpose of this policy is to provide guidance on the usage of information gathered offline or online from clients and employees.

1.3 Key Policies:

Data collections: Data are collected through any of the following channels

- Direct registration for our service (online/offline)
- Subscription to our email list.
- Attend or participate in online and/or in-person events.
- Contact us directly by email, phone, social media or other communications methods.
- Log data. Client's data can be store when they access or use our Websites or Services. This log data may include the Internet Protocol (IP) address, browser type and settings, the date and time the Services were used, and cookie data.

Use of Collected Information: We collect the following information in order to provide Client an exceptional service delivery which include PIN generation and continuous service delivery. All client data stored must aligned with the following:

- Fairness: All Processing of Personal Data must be fair, proportionate and compatible with the purposes for which the data were collected.
- Necessity: Personal Data are deleted when no longer needed.
- Security: Personal Data are protected by appropriate security measures.

Disclosure of Collected Information: Collected and stored information may be disclosed to Regulators and law enforcement agencies if there exist a valid reason to do so under the law guiding our service delivery.

While we strive to protect collected information and privacy, we cannot guarantee the security of any information that client disclose or transmit themselves and therefore and cannot be responsible for the theft, destruction, or inadvertent disclosure of such information.

Security of Collected Information

- Protection of Data in Transit: All our sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TSL etc) to protect the contents of data in transit.
- Network security using firewalls and network access control must always be up and running at all time to prevent data in transit against malware attacks or intrusions.

1.0 Objectives

- 1.1 This guidance is intended to supplement the FPL Information security policies, and to provide a clear procedure to handling data breach incidence.
- 1.2 To provide a process of reporting suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate personnel; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved and ensure that they are appropriately logged and managed in accordance with best practice.
- 1.3 This policy applies to all methods of processing of personal information, on any device, whether FPL or personally owned, which is used for the company purposes, whether, on a regular or an ad-hoc basis.

2.0 Scope

This policy covers all staff and computer systems, network devices, and any additional systems and outputs containing or transmitting FPL Protected Sensitive data.

3.0 Key Definition

A data security breach is considered to be “any loss of, or unauthorised access to, FPL’s data”.

Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential Data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceit
- For the purposes of this policy data security breaches include both confirmed and suspected incidents.

4.0 Key Policy - Breach of Data

- 4.1 A personal or sensitive data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the purposes of the Company’s business.

4.2 Members of staff, who access, hold or process personal or sensitive data for the purposes of the Company's business must take appropriate steps to ensure no unauthorised or unlawful processing, accidental loss, destruction of, or damage to personal data occurs.

4.3 A personal data breach can occur for a number of reasons, such as:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking attack;

This policy adopted a consistent approach to all reported data breach incidents, with the aim to ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by appropriately authorised and skilled personnel
- Incidents are recorded and documented
- The impact of the incidents is understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external Scrutiny
- External bodies or data subjects are informed as required
- The incidents are dealt with in a timely manner and normal operations restored
- The incidents are reviewed to identify improvements in policies and procedures.

5.0 Roles and Responsibilities

- IT & Systems Department: Where the incident / breach involves digital information or technical resources, ITSD will be responsible for the technical controls to support securing the network and containing or recovering the data.
- Risk Management Department: Will be responsible for overseeing management of the data breach incidence with a view to ascertain the impact of such on the business.
- Information users: All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

- Head of Department: The Heads, of the department/branch that uses the involved system or output or whose data may have been breached or exposed must comply and assist with investigations as required.
- Additional departments based on the data type involved, and as assigned by the ED, OP&S.

6.0 Containment and Recovery

6.1 Data security breaches should be contained and responded to immediately upon discovering the breach. An Impact Assessment should be undertaken to identify measures required to contain or limit potential damage, and recover from the incident.

6.1 All data breaches, actual and potential, must be reported to the Company through the IT & Systems Data Breach Incident Reporting Form, where appropriate.

7.0 Assessing the Risk

7.1 Some data security breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role (i.e. a laptop is irreparably damaged, but its files were backed up and can be recovered). Following immediate containment, the risks must be assessed which may be associated with the breach, potential adverse consequences to the individuals, as well as, the Company, and the seriousness of the breach must be considered, further to immediate containment and documentation.

7.2 The following must be considered upon discovering a data breach:

- The type of data involved;
- Whether the data is sensitive
- If data has been lost or stolen, whether encryption protections are in place;
- What has happened to the data, such as the possibility that it may be used to cause harm to the individual(s);
- The level of detail that would be exposed and how this could affect the individual

8.0 Notification of Data Breaches

8.1 Upon the completion of an Impact Assessment by IT & Systems and/or Risk Department, breaches capable of adversely affecting the individuals should be communicated to those individuals for the purposes of ensuring that specific and clear advice is provided on the steps to be taken to mitigate the risks and if any support could be provided.

8.2 Throughout the breach management process, records should be kept of what action has been taken, when and by whom. In addition, copies of any correspondence relating to the breach should be retained.

8.3 The ED, OP&S must be notified of all breaches that involve personal data.

8.4 Staff, vendors, consultants, and others who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

8.5 It must be evaluated whether the regulatory agencies, and/or other third parties such as the Police or bank should be notified of the data breach.

8.6 Serious breaches may require for a 'media message' to be communicated to individuals concerned and the public at large, dependent on the seriousness and extent of the breach, which should be considered and implemented where appropriate.

9.0 Evaluation and Response

9.1 It is important that data breaches, actual or potential, are documented and investigated, and the response to the breach is evaluated in terms of its effectiveness.

9.2 Where a breach is caused by systematic and ongoing problems, merely containing the breach and continuing 'business as usual' will not be deemed acceptable. Areas requiring improvement for the purposes of preventing a re-occurrence should be identified and Policies and Procedures updated or implemented, as appropriate.

Policy Code: FPL_IT_SP_22

Policy Name: Active Directory Domain Policy

Purpose: The purpose of this policy is to ensure that only properly registered and configured IT equipment is able to join the FPL domain, to improve the detection of vulnerable equipment and to enhance the manageability and security of Windows desktops and other devices connected to the company's network.

Audience: All users of computers running Microsoft Windows operating system, computers capable of interoperating with Windows domains and mobility devices that are connecting to FPL's network, including staff, vendors and affiliates.

Key Policy:

- Active Directory services at FPL include:
 - A single, consistent point of management for users, applications, and devices.
 - Simplified management and use of file and print services making network resources easier to find, configure and use.
 - A central control of authentication information to manage security services for internal desktop/laptop users and remote users.
 - A single sign-on to AD integrated network resources for users.
- Staff have access to the intranet and internet to undertake their assigned jobs and collaboration with other departments.
- All computers and mobility devices running a Microsoft Windows operating system or an operating system that interoperates with a Windows domain and that are connecting to FPL's networks are required to join the "FCMBPensions" domain.
- Native Windows authentication is used to control access to the FPL's IT services - this authentication is transparent to domain members who would otherwise be prompted for credentials when accessing services like Desktop PC, network drives and print queues.
- FPL policies and other actions, with regard to security settings, patch levels or operating parameters, will be applied and implemented on computers and mobility devices that have joined the domain.
- Exemptions to domain membership are conditional upon approval and certification by the Head IT & Systems.
- All computers and mobility devices that are members of the FPL Windows domain must have the "Domain Admins" group as a member of the local Administrators group. When Windows computers join the domain, this group is automatically added; it must not be deleted subsequently.
- Domain Admins group access is required to verify service pack and patch levels, virus definitions, software versions and (where necessary) to purge or remove virus infections.

- ITS will create an account in the Windows domain for computer equipment and mobility devices when these are entered into the Network Administration System (NAS) database. When this equipment is configured to join the domain, it will then be associated with its pre-existing entry.
- All workstations joining the domain shall inherit all settings and rules already defined for the domain (e.g. USB block, CD Drive block, Wallpaper, Windows lock, Password rules and expiration setting etc) once the system is added to the network. Exception can only be given by Head, IT & Systems (e.g. for MD/CEO).
- IT & Systems reserves the right to temporarily or permanently deny access to any computer account, or other network resource that has been misused. This includes but not limited to, account/password sharing, non-official usage, false ownership or identification misrepresentation, malicious or unauthorized hacking and/or intrusion, electronic harassment, making unauthorized copies of any copyright protected software.

Purpose

The purpose of this policy is to ensure that access to ITS's Data Centres (including DR) is restricted to ensure safety and integrity of FPL data and the infrastructure stored in the data centres.

Applicable to: These guidelines apply to all parties who wish to access the FPL data centres.

Key Policy

1. Access to Data Centres will be granted to the following groups and Access Control Specifications.

(a) Group A:

- IT permanent staffs whose role stipulates that they are responsible for operating and / or maintaining the data centre and / or its equipment.
 - Access Control Specifications for Group A: Work requiring access to the data centres should wherever practical be scheduled between 8:00am and 5:00pm Monday – Friday. Exceptions to this requirement are granted to the group where necessary (e.g. Late/Early office hour work and weekends) as may be instructed by Head, IT & Systems or his Deputy.

(b) Group B:

- People who require access to the data centres to maintain or service specific equipment in the data centre. This group includes (Suppliers, selected vendor, service engineers etc.)
 - Access Control Specifications for Group B: Access to data centres is permitted while accompanied by a member of Group A (i.e., as long as someone from Group A is present for the duration of the visit) and a physical success log must be sign in and off by the said group B member.
 - Access will normally be limited to between 8:30am and 5:00pm Monday – Friday and sometimes weekend as approved by the Head, IT & Systems.

(c) Group C:

- Staff on induction, will be allow to enter the data centre as per Corporate Resources induction notification.
- Interested Parties (Clients, Partners, Directors etc) who are interested in the data centres may request a guided tour upon instructions from the Executive Directors, Operations and Services (ED, O&S)
 - Access Control Specifications for Group C: Access by this group upon receiving notification from ED, O&S will be allowed once and they will be required to sign in the access log.

- Access is granted only when such visits will not compromise efficient operations of the data centre.

2. After Hours Access: Any planned access (outside normal hours) must be pre-approved by the Head, ITS.

3. Urgent Access: Where access is required in an Emergency, Group A members may access the data centre in an emergency. Any urgent access will be considered a significant event. An incident log will be completed by the assigned IT & Systems staff.

4. General Rules for Access

Anyone permitted access to the data centres will adhere to Procedure and Guidelines for Safely Performing Work in an Active Data Centre (including cleanliness). These procedures are attached as Appendix B. These procedures may be updated periodically by the Manager, Operations Services.

Policy Code: FPL_IT_SP_24

Policy Name: Vulnerability Management Policy

Policy Statement

This control procedure defines the ITS approach to threat and vulnerability management, and directly supports the following policy statement from the Information Security Policy:

The IT & Systems will ensure the correct and secure operations of information processing systems.

Frequency

The vulnerability assessment test for FCMB Pensions shall be carried out on an annual basis. With all the activities and vulnerability methodology outsourced to a 3rd party vendor. No vendor will undertake the vulnerability assessment for more than two consecutive years.

Audience

This procedure is intended to be read and understood by IT & Systems staff who are responsible for the management of IT systems

Scope and Frequency of Vulnerability Assessment

- Protective monitoring
- Client anti-virus
- Server anti-virus
- Use of external vulnerability assessment
- Software versions
- Client patching
- Server patching
- Firmware patching

1. Protective Monitoring

All network connection is currently being monitored and every user is expected to login to the tool before they can perform network critical task. User access level control is in place to effectively report user's activities. This is available daily.

2. Client anti-virus

All IT & Systems-managed clients run endpoint protection. Updates are pulled to a management server and clients check for updates every ten minutes. Where signatures are released to address a critical threat, the updates can be deployed at short notice and outside of normal schedules.

3. Server anti-virus

Signatures are made available.

4. Use of external vulnerability assessment

The IT & Systems will use external vulnerability assessments to supplement its internal capabilities at least once a year. The penetration testing will include all internal and external facing services. Decisions to use external vulnerability assessments will be made and authorised by ED-Operations and Services.

5. Software versions

Where possible the ITS will run the latest stable version of software, and no older than the previous version provided that it remains supported, in order to maintain stability, supportability and security. Where compatibility issues prevent running the latest version, the IT & Systems will prioritise upgrading or replacing the component causing the compatibility issue. Where legacy systems have to be tolerated, its Cyber Security impact needs to be ascertained before retaining such systems. Where there is no appropriate treatment, ITS reserve the right to disable software and services deemed to present a significant risk to the systems or data.

6. Client patching

All IT & Systems-managed Windows clients receive Windows updates on a monthly basis. Key third party software – including browsers, Flash plug-in and Adobe Reader – are also updated on need base requirement. Where patches are released to address a critical vulnerability, they can be deployed at short notice and outside of normal schedules. (See Patch Management Policy)

7. Server patching

All Windows servers are included in a rolling monthly patch schedule or in some cases patched manually where there is greater risk for disruption. Where patches are released to address a critical vulnerability, they can be deployed at short notice and outside of normal schedules. All databases will be patched as required, using the appropriate tools for MS SQL, MySQL.

8. Firmware patching

Where possible the ITS will run the latest stable version of firmware, and no older than the previous version provided that it is supported, in order to maintain stability, supportability and security. Where compatibility issues prevent running the latest version, the ITS will prioritise upgrading or replacing the component causing the compatibility issue.

Roles and Responsibilities

The System Administrator will coordinate the execution of the Vulnerability management policy.

INTRODUCTION

FCMB Pensions Limited operates a Circuit Television System (CCTV System) within its premises. This policy details the purpose, use and management of the CCTV system within the premises. This policy applies to all CCTV systems operational within the premises of the Company. The Company will observe the provisions of the Nigeria Data Protection Regulation 2019 and other relevant laws including Freedom of Information Act 2011 in its operation of system.

SCOPE

The Company has CCTV systems installed at the entrance of the Company, the reception, the Entrance gate, the sides of the building, within the corridors of the Company but not in the offices where employees stay. The CCTV is operational for 24 hours a day, every day of the year. The cameras are monitored in the IT room which is secure and not accessed by unauthorized persons. The whole operation of the CCTV is in accordance with the Nigeria Data Protection Regulation 2019.

PURPOSE OF THE CCTV

The CCTV are installed for the following reasons:

- For crime prevention, detection and investigation.
- To ensure safety of employees and other staff
- To ensure security and protection of clients' personal information and Company's property.

The installed CCTV will monitor the Company's premises and identify incidents that will require attention and response. This surveillance will be undertaken in a manner that will respect the fundamental rights and freedom of individuals.

LAWFUL BASIS

Our lawful justification for deploying these CCTV is our legitimate interest to protect our employees, staff, services, premises and client information. We have assessed our legitimate interest and have arrived at the conclusion that there is balance of interest in the processing activities.

RETENTION PERIOD

We only keep CCTV images for a specified period of time. Except where required for evidential purpose, investigation of offence or by law to be kept for longer period, we will only retain the CCTV image no longer than 3 months from the date of recording. The images will be overwritten after this period. Images held in excess of the retention period will be reviewed occasionally to determine the necessity and proportionality of retaining them. Access to CCTV image is restricted to only authorized persons.

DISCLOSURE OF CCTV IMAGES TO THIRD PERSON

We may disclose the CCTV footage to a third in the following limited circumstances such where disclosure is required by law for the purpose of preventing or detecting crime, where sought as evidence by investigating officer in relation to a crime committed in our premises.

SECURITY MEASURES

We have put implemented adequate technical and organizational measures to prevent any unauthorized access, disclosure, alteration, accidental losses or destruction of the CCTV footage. These includes putting in place a password activated door to where the CCTV system resides, encrypting the storing and transmission of the footage, using password protection to limit access to the CCTV footage and conducting regular audit.

COMPLAINT PROCEDURE

All complaint concerning the use of CCTV or its disclosure should be made to IT&systems@fcmbpensions.com or send a letter to our physical office @ 207 Zakaria Maimalari Street, Cadastral Zone AO, CBD

POLICY REVIEW

This policy will be updated occasionally to comply with relevant provisions of law and to accommodate new development in the use of our CCTV.

Introduction

FCMB Pensions Laptop Computer policies apply to the use of all laptop systems inside and outside the office premises and staff members are expected to follow all of these policies when using the FCMB Pensions laptop computers.

Aim

FCMB Pensions has decided to allow staff to use the FCMB Pensions laptop computers inside and outside the company in order to enhance, enrich, and efficiently make staff productive anywhere and at any time.

Allocation

FCMB Pensions laptops are to be used as a productivity tool for PFA business. Staff members may use the FCMB Pensions laptops for limited personal purposes subject to this policy, however staff members also shall exercise appropriate professional judgment and common sense when using the FCMB Pensions laptop computers. All laptops and related equipment and accessories are FCMB Pensions property and are provided to the staff members for a period of time as deemed appropriate by the company through IT & Systems Department

Laptop Computer Usage

As a condition of their use of the FCMB Pensions laptop computers, staff members must comply with and agree to all of the following:

- I. Prior to being issued one of the FCMB Pensions laptop computers, staff members will sign the Laptop allocation Form and agree to all outlined policies.
- II. Staff members should NOT attempt to install software or hardware or change the system configuration including network settings without prior consultation with IT & Systems Department.
- III. Staff members are expected to protect Company laptops from damage and theft.
- IV. Each staff member is monetarily responsible for any hardware damage that occurs off company premises and/or software damage (including labour costs).
- V. Staff members will not be held responsible for computer problems resulting from regular company-related use; however, staff members will be held personally responsible for any problems caused by their negligence as deemed by FCMB Pensions IT & systems.
- VI. Staff members will provide access to any laptop computer, equipment, and/or accessories they have been assigned upon.

General Laptop Use Rules

- I. Important data on the laptop must be backed up on your network folder as a safety precaution against hard drive failure. The seconds that it takes to create a backup are well worth the frustration if/when the computer hard disk fails.
- II. Since the laptop's keyboard and touch pad are permanently attached to the rest of the system, make sure that your hands are clean before using them. Because hand lotion is a major contributing factor to dirt and dust, please make sure your hands are free from lotion before using the computer. It is costly to change a laptop keyboard and/or touch pad that has been damaged by excessive dirt.
- III. Do not place drinks or food in close proximity to your laptop.
- IV. Extreme temperatures or sudden changes in temperature can damage a laptop. You should NOT leave a laptop in an unattended vehicle. When using the laptop, keep it on a flat, solid surface so that air can circulate through it. For example, using the laptop while it is directly on a bed can cause damage due to overheating.
- V. ALWAYS keep your laptop plugged into the supplied surge protector when it is plugged in or charging.

How to Avoid Laptop Computer Theft

Due to size and portability, laptop computers are especially vulnerable to theft. Staff members should follow the rules set out below.

- I. Do not leave a laptop in an unlocked vehicle, even if the vehicle is in your driveway or garage. Never leave it in plain sight. If you must leave your laptop in a vehicle, the best place is in a locked trunk. If you do not have a trunk, cover it and lock the doors.
- II. Be aware of the damage extreme temperature can cause to computers.
- III. Carry your laptop in a nondescript carrying case or bag when traveling.
- IV. Do not leave a meeting or conference room without your laptop. Take it with you.
- V. Never check a laptop as luggage at the airport.
- VI. Lock the laptop in your office or classroom during off-hours or in a locked cabinet or desk when possible. If a theft does occur, immediately notify FCMB Corporate Resources Department or IT & Systems Department.

APPENDIX

EMPLOYEE’S WORK FROM HOME FORM

EMPLOYEE NAME	
DEPARTMENT/BRANCH	
DATE REQUESTED	
JUSTIFICATION OF YOUR REQUEST	
Personal Laptop/Official Laptop	<i>Please provide as much information as possible:</i>
Are you aware of remote work ethics?	
Can you ensure security of the company’s data in the course of working remotely?	
HOD’S JUSTIFICATION	
Kindly provide justification for your approval	
CONFIDENTIALITY STATEMENT:	
I hereby agreed that “Technical and Company information” relating to my work, company’s Products and services, software, finances and strategies, client’s information, and current or future business plans and models, shall not be compromised in any form through unauthorize access.	
Signature:	Date:
ED, OPERATIONS & SERVICES’ APPROVAL	
Comments:	
Signature:	Date:



FCMB PENSIONS LIMITED
VENDOR PERFORMANCE EVALUATION FORM
 (To be filled by IT & Systems Department)

Instructions: This form is to be used by IT & Systems department to evaluate the overall performance of vendors we are currently working with. Include all information associated with the vendor and apply a performance rating. Definitions are provided below. Vendor performance evaluations are recommended for all vendors to report all levels of service (exceptional, satisfactory, cautionary or unsatisfactory). Vendors receiving an overall unsatisfactory rating will be informed of the rating.

Vendor Name:		Product/Service Name:
Date:	Signature:	Deployed Department:

DEFINITIONS OF PERFORMANCE RATINGS

EXCEPTIONAL (9 – 10) Exceeds contractual requirements. The actions taken by the vendor met the	Good (7 – 8) Meets contractual requirements. The actions taken by the vendor were very effective	SATISFACTORY (5 – 6) Meets contractual requirements. The actions taken by the vendor were	CAUTIONARY (3 - 4) Does not meet contractual requirements. The action taken by the vendor is of minor	UNSATISFACTORY (0 – 2) Does not meet contractual requirements, and recovery is not likely in a timely manner. The vendor's
--	--	---	---	--

PERFORMANCE RATING	Actual Scores	COMMENTS (Attach additional sheets if
Product/service delivered and worked as expected with less issue and in compliance with contract terms.	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Availability of experienced and stable support staff	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Prompt and effective correction of situations and issues	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Product stability, responsiveness and scalability	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Documentation records, manuals and receipts received in a timely manner and in compliance with contract specifications	<input type="checkbox"/> Exceptional <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Total	/50	

OVERALL PERFORMANCE

Exceptional (45-50)

Good (35-44)

Satisfactory (25-34)

Cautionary (15-24)

Unsatisfactory (0-14)

***Resolutions for unsatisfactory performance should be documented in the vendor reply section below and should be reviewed by the Audit Department.**



FCMB PENSIONS LIMITED
VENDOR PERFORMANCE EVALUATION
 (To be filled by the deployed department if applicable)

Instructions: This section is to be filled by the department using the product/services whose vendor is being review. Definitions are provided below. Vendor performance evaluations are recommended for all vendors to report all levels of service (exceptional, satisfactory, cautionary or unsatisfactory). Vendors receiving an overall unsatisfactory rating will be informed of the rating and they will be provided a reasonable opportunity to respond.

Product/Service Name:	Deployed Department:	Signature:
Staff:	Date:	

DEFINITIONS OF PERFORMANCE RATINGS

EXCEPTIONAL (9 – 10) Exceeds user’s expectation. The application met the user’s requirements and the scope of services were	Good (7 – 8) Meets user’s requirements. The application performance is good.	SATISFACTORY (5 – 6) The application response vendor were Satisfactory	CAUTIONARY (3 - 4) The application is slightly below expectation.	UNSATISFACTORY (0 – 2) The application was very ineffective.
---	--	--	---	--

PERFORMANCE RATING	Actual Scores (2-10)	COMMENTS (Attach additional sheets if
General impressions of software and responsiveness.	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Product features and relevance	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Reporting functionality and accuracy of output.	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Product stability and frequency of issues.	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Product usability and learnability.	<input type="checkbox"/> Exceptional <input type="checkbox"/> Good <input type="checkbox"/> Satisfactory <input type="checkbox"/> Cautionary <input type="checkbox"/> Unsatisfactory	
Total	_____/50	

OVERALL PERFORMANCE

Exceptional (45-50)
 Good (35-44)
 Satisfactory (25-34)
 Cautionary (15-24)

Unsatisfactory (0-14)

***Resolutions for unsatisfactory performance should be documented in the vendor reply section below and should be reviewed by the Audit Department.**

Auditor: _____ **Signature:** _____

Date: _____



**INFORMATION TECHNOLOGY & SYSTEMS DEPARTMENT
VENDOR ONBOARDING FORM**

PENSIONS

Company Name		
Address		
Contact Person		
Mobile Number		
Nature of Service (please mark as appropriate)		
Hardware	Software	Communication/Networking
Date Service Started		

S/N	Service Description	Purpose

For Internal Usage Only

Documented By:

Approved by:

Name: _____

Name: _____

Signature: _____

Signature: _____

Date: _____

Date: _____

VENDOR'S PERSONAL IDENTIFICATION INVENTORY

S/N	VENDORS	SERVICES RENDERED	CONTACT PERSON	CONTACT ADDRESS
1	CPAAT CONSULTING LIMITED	SERVICE HELPDESK SOLUTION	Aysha Abdullahi 08097111801 aysha.abdullahi@cpaat-consulting.com	Phase 1, 4 Fola Jinadu Cres, Gbagada, Lagos
2	SIMPLEX SYSTEMS LTD	IBSPCC/MONEYTOR, QLIKVIEW	Femi Adeniyi 08022235852	28, Gbolade Adebanjo street, Ilupeju, Lagos.
3	BUSICON NIGERIA LTD	DOCUWARE	Ayodeji 07039270800	697 Idris Gidado St, Wuye 900108, Abuja
4	STAUNCH TECHNOLOGIES	DOMAIN SECURITY	Issa Ajao 08033011305 Easy4issy@gmail.com	No 22B Babatunde Anjous Street, Lekki phase 1. Lagos.
5	TISV	WEBSITE MAINTENANCE	Omotolani Tayo-osikoya 09098108427	1/3 Ekolu Street Surulere, Lagos.
6	INTELLIGENT NETWORK	IVR CALL CENTER, LEGEND CRM	Gbolahan 08023175974 Tolani@tisvdigital.com	4, Fola Jinadu Crescent, Gbagada Estate Phase 1, Gbagada, Lagos.
7	ACCORD CUSTOMER CARE SOLUTION (ACCS)	DATA DOMAIN	Folarin Banigbe 08035200347	7, Asiata Solarin Crescent, Off Kudirat Abiola Way, Oregun Lagos.
8	CHUKS AZOGU	SAGE (EVOLUION AND PAYROLL)	Chuks Azogu 08187206558	No 3 King Perekule GRA Port-harcourt.
9	PACIFIC SOLUTION AND TECHNOLOGY	CYBEROAM	Practul Kamar 08050693333	27A Alh. G. Kola Oseni St, Ilupeju, Lagos
10	AIRTEL	SECONDARY INTERNET LINK	Joanna 08022228022 Alfred 07056477023	
11	INQ LTD.	PRIMARY INTERNET LINK	Oje Ozolua Imokhuede 09096740212 imoukhede.oje-ozolua@inq.inc	3A, Aja Nwachukwu Street, Ikoyi, Lagos.
12	SOFT SOLUTIONS LIMITED	ANTIVIRUS(McaFEE)	Oluwafemi Odeyemi 08033999307	16A Residence Road, LGA, Gbagada
13	DYNATECH	SMS PROVISION	Ahmad	Suite 5 Febson Mall Old Russel Centre Wuse zone 4, Abuja

			08037896855 info@dynatech.com.ng	
14	ALLIED COMPUTERS	HITACHI SAN STORAGE	Babatunde Kassim 7081321192	Zone 4, Suite 5, Hilltop House, Wuse, Gwani St, Wuse, Abuja,
15	FOXFIRE LIMITED	COMMUNICATION/ SURVEILLANCE	Tabs Odukwe 7038487073	1381-1393 Aminu Kano Cres, Wuse 904101, Abuja
16	REELTECH BUSINESS SOLUTION	MS NAV	Yetunde Adeleye 8059194415 Dejiolaofe@reeltechsolutions.com	2 Oyetola Idowu St, Ilupeju, Lagos
17	SOFT SOLUTIONS CONCEPT LIMITED	HR WORKPLACE	Abayomi Oyenibi 08021810040 info@focusgroup.com	Faith house, Plot75, Block 15, Ichie Mike Ejezie, Off Fola Isibo. Lekki Phase 1, Lagos.

DATA BREACH INCIDENT REPORTING FORM

NAME OF PERSON REPORTING:	DATE OF BREACH OCCURRING:	DATE DATA BREACH WAS DISCOVERED:
	TIME:	TIME:
DEPARTMENT/BRANCH		
MOBILE NUMBER:		
DETAILS OF THE DATA BREACH		
How did the breach occur?	<i>Please provide as much information as possible:</i>	
Has a breach of this nature occurred before within the Department/Branch?	<i>If so, please provide dates of any previous breaches of the same nature:</i>	
How many individuals does the data breach affect?	<i>Please, aim to provide a figure as accurate as possible:</i>	
Are the individuals affected by the breach clients/staff, or both?		
What data has been lost/stolen/compromised or else disclosed without the appropriate authority?	<i>i.e. Client's details, Financial information, Staff details etc.:</i>	
Whom was the data released to, if known?		
Is the data sensitive? YES/NO	<i>If YES, please provide a list of sensitive data concerned:</i>	
Are you aware of the individuals affected?	<i>If so, please provide their names and any contact details, where known:</i>	
What steps could those individuals take to protect themselves from any harm/risk arising from the breach?	<i>i.e. report to law enforcement, Auditor, Risk manager, ITSD etc.:</i>	
Does the breach concern manual or electronic data, or both?		
Were encryption protections in place at the time of the breach?		

Have the IT & Systems been informed?	<i>If your account has been hacked, you must change your password immediately and report the incident to IT & Systems:</i>
Has the incident been reported to the Police / any other authorities?	<i>If so, please provide date of reporting and reference number:</i>
IS THERE ANYTHING ELSE FCMB PENSIONS SHOULD BE AWARE OF?	
<i>Please comment below:</i>	
THIS FORM MUST BE SUBMITTED TO it&systems@fcmbpensions.com	

DETAILED INFORMATION SECURITY

INTRODUCTION

The FCMB Pensions Policy on Information Security requires the company to establish and maintain a documented Information Security Management (ISM). This shall address the assets to be protected, the organisation's approach to risk management, the control objectives and controls, and the degree of assurance required.

Information Security Policy

The information Security policy of FCMB Pensions LTD is designed to preserve:

- ❑ **Confidentiality:** ensuring that information is accessible to only those authorised to have access;
- ❑ **Integrity:** safeguarding the accuracy and completeness of information and processing methods;
- ❑ **Availability:** ensuring that authorised users have access to information and associated assets when required.

As part of this process each organisational unit must ensure that unit-specific security requirements, e.g. required by national regulations, are also included in the 'statement of applicability'. This policy document shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate.

The FCMB PENSIONS ITSC will be responsible for review and evaluation of the policy.

- The policy will be reviewed following any significant security incidents.
- The policy will be reviewed at least annually.
- The review of the policy will include:
 - The continued effectiveness of the policy in the light of incidents occurring
 - The scope of the policy in the context of new business operations, acquisitions, disposals or mergers
 - The continued cost effectiveness and fitness for purpose of the controls flowing from the policy

Scope of ISM

This Information Security Management is applicable to the complete organisation, all locations, all business applications, information processing facilities, networks, and application development functions, belonging to FCMB Pensions. For elements of the business processes not under direct control of the Operations Group or Information Technology department, detailed contracts must be available, clearly defining security responsibilities for these elements.

- Business profile: Short overview of the major business processes of FCMB Pensions, the critical applications and IT infrastructure supporting these processes, the organisation structure, and the major locations of FCMB Pensions.
- Risk assessment: The information assets of FCMB Pensions business can generally be classified, related to the different security aspects, as follows:
 - Confidentiality: Business information assets may contain sensitive customer related information which could be very harmful to both FCMB Pensions and the customer if exposed to the public or competitors. It needs to be protected against exposure.
 - Integrity: Business information assets, if corrupted or fraudulently misused, may cause serious damage to FCMB Pensions and/or its customers; integrity of critical data needs to be guaranteed.
 - Availability: Business activities may be very time-critical; supporting IT functions must ensure that those time-critical activities can continue when business needs it.
 - Business growth: The information risk level has been risen significantly because of the fast growth of the business in recent years. This requires clear assignments of responsibilities and restricted access to information assets by employees with a need to know only.
 - Legal requirement: Government regulations require good protection of customer information and compliance with legal requirements.
 - Risk management: Significant risks are most likely to exist in:
 - Business continuity arrangements
 - Management approved authorisation to access/handle information assets.
 - Security management system: a clear management commitment to secure Business unit information assets. Planned improvement actions will focus on these areas in particular, but more generally, FCMB Pensions intends to operate a program that will ensure adequate protection of all information assets.

- Critical assets will have designated owners; owners need to be fully aware of their responsibilities to protect FCMB Pensions and customer data in relation to its importance.

Information Security – Roles and Responsibilities

The Head of Department is responsible for implementation of the policy principles. These responsibilities include publishing of this document on the intranet; management must ensure that all staff are aware of their obligations, in particular:

- To comply with all relevant legislation and compliance requirements whether internal or external
- That IT facilities may only be used in a secure manner and for authorised purposes only.
- That all use of proprietary software must be in accordance with the licence terms and conditions
- That staff must never disclose their passwords
- Security incidents need to be reported to management
- To better structure the Information Security management process, the following specific Roles and Responsibilities regarding Information Security have been defined:

Info Security Director

The MD/CEO of FCMB Pensions will be the Information Security Director. While the Head of IT will be responsible for availability, integrity and confidentiality of the Information assets and IT processes of FCMB PENSIONS.

Info Security Coordinator

The Head of IT in Liaising with the ED will be responsible for coordinating information security. Collectively they should:

- Support and advise senior management in the discharge of their responsibilities as it relates to information security.
- Develop appropriate information security policies and principles
- Have ownership of and responsibility for the information security education and training program
- Investigate as requested by senior management
- Receive reports of any security incidents
- Ensure that the information security process is implemented satisfactorily

- Liaise with appropriate information security specialists outside the company
- Promote the adoption of information security controls and principles that are cost effective and fit for purpose
- Support and facilitate the risk assessment process for the unit
- Advise the ITSC to select appropriate controls, prepare a relevant statement of applicability, and maintain the policy document

Information Security Controls

Objective: To manage information security within the organisation.

- Allocation of Responsibilities: Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.
- Authorization Process: A management authorisation process for new information processing facilities shall be established.
- Co-operation: Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.
- Inventory of Assets: An inventory of all important assets shall be drawn up and maintained.

User Training

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

- Information security education and training: All employees of the organisation shall receive appropriate training and regular updates in organisational policies and procedures.

Responding to Security Incidents and Malfunctions

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

- Reporting Security Incidents: Security incidents shall be reported through appropriate management channels as soon after the incident is discovered as possible.
- Disciplinary Process: The violation of organisational security policies and procedures by employees shall be dealt with through a formal disciplinary process.

Physical and Environmental Security

Objective: To prevent unauthorised access, damage and interference to business premises and information.

- Physical Security Perimeter: Organisations shall use security perimeters to protect areas which contain information processing facilities.
- Physical Entry Controls: Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access (I.e. Biometric Door).
- Working in Secure Areas: Additional controls and guidelines for working in secure areas shall be used to enhance the security provided by the physical controls protecting the secure areas.
- Isolated Delivery and Loading Areas: Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

Equipment Security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

- Equipment Siting and Protection: Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
- Power Supplies: Equipment shall be protected from power failures and other electrical anomalies.
- Cabling Security: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
- Equipment Maintenance: Equipment shall be maintained in accordance with manufacturer's instructions and/or documented procedures to ensure its continued availability and integrity.
- Disposal or Re-use of Equipment: Information shall be erased from equipment prior to disposal or re-use.

System Planning and Acceptance

Objective: To minimise the risk of systems failure.

- Capacity planning: Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
- System acceptance: Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.
- Protection against malicious software: Objective: To protect the integrity of software and information.

- Controls against malicious software: Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.

Housekeeping

Objective: To maintain the integrity and availability of information processing and communication services.

- Information back-up: Back-up copies of essential business information and software shall be taken daily.
- Fault logging: Faults shall be reported and corrective action taken.

Network Management

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

- Network Controls: A range of controls shall be implemented to achieve and maintain security in networks.

Media Handling and Security

Objective: To prevent damage to assets and interruptions to business activities.

- Management of Removable Computer media: The management of removable computer media, such as tapes, disks, and printed reports shall be controlled.
- Disposal of Media: Media shall be disposed of securely and safely when no longer required.
- Information Handling Procedures: Procedures for the handling and storage of information shall be established in order to protect such information from unauthorised disclosure or misuse.
- Security of System Documentation: System documentation shall be protected from unauthorised access.

User Access Management

Objective: To prevent unauthorised access to information systems.

- User registration: There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.
- Privilege management: The allocation and use of privileges shall be restricted and controlled.

- User password management: The allocation of passwords shall be controlled through a formal management process.
- Review of user access rights: A formal process shall be conducted at regular intervals to review users' access rights.

User Responsibilities

Objective: To prevent unauthorised user access.

- Password use: Users shall be required to follow good security practices in the selection and use of passwords as detailed in the Password Security Standards.
- Unattended user equipment: Users shall be required to ensure that unattended equipment has appropriate protection by ensuring such equipment is locked.
- User authentication for external connections: Access by remote users shall be subject to authentication.

Application Access Control

Objective: To prevent unauthorised access to information held in information systems.

- Information access restriction: Access to information and application system functions shall be restricted in accordance with the access control policy.

Monitoring system access and use

Objective: To detect unauthorised activities.

- Event logging: Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
- Monitoring system use: Procedures for monitoring use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.


CONTROL PAGE

Approval Dates: 17/06/2013
16/12/2014
29/03/2016
21/09/2017
28/04/2019

APPROVAL PAGE

Head, IT and Systems		Date: 21/11/14
Chairman ITSC		Date: 21/11/14
MD/CEO		Date: 16/12/14
Chairman, Risk Committee		Date: 16/12/14
Chairman BoD.		Date: 16/12/2014

APPROVAL PAGE


Head of IT and Systems

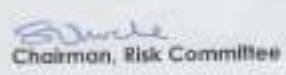
Date: 29/03/2016


Chairman ITSC


Date: 29/3/16


MD/CEO

Date: 31/3/16


Chairman, Risk Committee


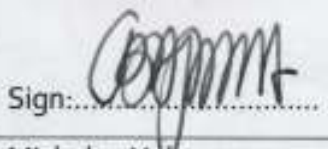



Date: 26/5/16


Chairman BOD




Date: 26/05/2016

DEPARTMENT	IT & SYSTEMS DEPARTMENT
TITLE OF DOCUMENT:	IT & SYSTEMS DEPARTMENT STRATEGY DOCUMENT
	<u>Approved by:</u>
AUTHOR / PREPARED BY:	Luloman Yusuf Designation: Head, IT & Systems Department Date: 20/09/2017 Sign: 
EXECUTIVE MANAGEMENT	Christopher B. Bajawa Designation: Executive Director, Operations & Services Date: 20/09/2017 Sign: 
MANAGING DIRECTOR/CEO	Misbahu Umar Yola Date: 20/9/17 Sign: 
CHAIRMAN BOARD RISK MANAGEMENT COMMITTEE	Date: 21/9/17 Sign: 
BOARD CHAIRMAN	Date: 21/9/17 Sign: 

APPROVAL PAGE

IT & SYSTEMS DEPARTMENT	
Designation	
Head, IT & Systems Department	Lukman Yusuf Sign:  Date: 01/04/19
Executive Director, Operations & Services	Christopher Bajowa Sign:  Date: 18/4/19
Managing Director/CEO	Misbahu Yola Sign:  Date: 18/04/19
Chairman, Board Risk Management Committee	Suzanne Iroche Sign:  Date: 30/7/19
Chairman, Board of Directors	Ladi Balogun Sign:  Date: 30/7/19

APPROVAL PAGE

IT & SYSTEMS DEPARTMENT	
Designation	
Head, IT & Systems Department	<p>Lukman Yusuf</p> <p>Sign:  Date: 20/7/19</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>

APPROVAL PAGE

IT & SYSTEMS DEPARTMENT

Designation	
Head, IT & Systems Department	Lukman Yusuf Signature..... Date.....
Executive Director, BD & Investment	Mai Mustapha Signature..... Date.....
Managing Director/CEO	Christopher Bajowa Signature..... Date.....
Chairman, Board Risk Management Committee	Caroline Anyanwu Signature..... Date.....
Chairman, Board of Directors	Ladi Balogun Signature..... Date.....