Nigeria Cloud Computing Policy

National Information Technology Development Agency

(NITDA)

August, 2019

CONTENT

POLICY HISTORY

S/N	Author	Version No	Release Date	Change Details	
1.	NITDA	1.0	April, 2019	First Draft Review by NITDA	NITDA
2.	NITDA	1.1	May, 2019	Second Review by Stakeholders	Stakeholders
3.	NITDA	1.2	July, 2019	Third Review by NITDA and Stakeholders	Stakeholders & NITDA

POLICY METADATA

S/N	Data Elements	Values
1.	**Title**	National Cloud Computing Policy
	Title Alternative	NGEA
2.	**Document Identifier**	NIG-NITDA.13
3.	**Document Version, month, year of release**	Version 1.2; August, 2019
4.	**Publisher**	National Information Technology Development Agency (NITDA)
5.	**Type of Regulation Document** *(Standard/ Policy/ Technical Specification/ Best Practice /Guideline / Framework /Policy Framework/Procedure)*	Policy
6.	Enforcement Category *(Mandatory/Recommended)*	Recommended
7.	Owner of approved regulation	NITDA
8.	Target Audience	A Public Institutions (including Local, State and Federal Government); ICT Product/Service Providers for public institutions; SMEs for public institution; Professional Bodies; Development Partners; and General Public.
9.	Copyrights	NITDA
10.	Format *(PDF/A at the time of release of final Regulation)*	PDF
11.	Subject *(Major area of Standardization)*	Cloud Computing

Foreword

The country socio-economic activities and businesses are increasingly dependent on Information Communication Technology (ICT). The need to make these computing resources available and accessible is critical to the country's continuous growth and sustainable development. The country's Economic Recovery and Growth Plan (ERGP) recognizes information technologies as an enabler for promoting a digital-led growth. Digital-led growth cannot happen except the country has policy direction peculiar to her environment for supporting the government and SMEs to acquire and deploy computing resources in the most efficient manner.

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service interaction.

Adoption of Cloud Computing policy by Nigerian Government will lead to capital costs reduction, improved responsiveness to citizens' or customers' needs, increased transparency and enhanced public service delivery. In addition, cloud computing adoption will also support Small Medium Enterprise (SMEs) that provide IT-enabled services to the government cross the barrier of initial IT capital investments and ensure there is a provision suitable for cloud procurement in the country's procurement requirements. This will facilitate creation of new set of jobs and add value to the economy.

Therefore, the Nigeria Cloud Computing Policy (NCCP) is promoting "Cloud First" as a proposition to Federal Public Institutions (FPIs) and SMEs as an efficient way of acquiring and deploying computing resources for better and improved quality of digital services.

Dr Isa Ali Ibrahim (Pantami), PhD, FNCS, FBCS, FIIM
Director General/CEO,
National Information Technology Development Agency (NITDA)
August, 2019.

DEFINITION

Small Medium and Enterprises (SMEs): refers to enterprises which have an annual turnover not exceeding Five Hundred Thousand Naira (N500,000).

Public Institutions (PIs): means Ministries, Departments, Extra-Ministerial Departments and Agencies of Government at Federal, State and Area Council levels.

Federal Public Institutions (FPIs): means Ministries, Departments, Extra-Ministerial Departments and Agencies of Government at the Federal level.

Cloud Computing: refers to computing model for ubiquitous, convenient, on-demand and real time network access pool of configurable and rapidly provisioned computing resources (networks, servers, storage, applications and services among others) required by and available to FPIs and SMEs to carry out their businesses and operations.

Cloud First Policy: refers to the Federal Government of Nigeria's strong commitment and support for cloud computing service adoption, especially from a local cloud service providers, as a first choice consideration while deploying and accessing computing resources in the public sector and by the SMEs that provide computing services to the public sector.

Government Data: Data produced or commissioned by government or government controlled entities.

Federal Open Data Initiative: refers to an initiative of the Federal Government through the Federal Ministry of Communications (FMC) aimed at ensuring substantial amount of public and non-sensitive data is released and used through digital platforms for the creation of innovative digital services that promote the country's social-economic development.

Cloud Migration: refers to the process of moving data, applications, hardware, software, network infrastructure and/or other business elements and services to a cloud computing environment.

Cloud Adoption: refers to the process or strategy that provides incentives for the public institutions and SMEs to use the cloud computing for their computing requirements in way that is efficient and sustainable.

Artificial Intelligence (AI): connotes the creation of intelligent objects that work and react like humans to carry out certain tasks meant for intelligent beings without human intervention.

Machine Learning (ML): connotes algorithm and programming that provides AI the ability to detect patterns in the data presented by smart systems, so as to learn from these patterns and improve actions from experience without human intervention

Internet of Things (IoTs): refers to the combination of concepts and technologies for embedding computer systems and the internet into all the artifacts/physical things in the real world in order to automatically collect, communicate and exchange data with one another through digital platforms. The digital platforms have ability to analyse the data and assist humans in automatic decision-making and action-taking

Virtualization: refers to the concepts and technologies that allow creation of a virtual version of a device or resource, such as server, storage device, network or operating system through a framework that divides the resource into one or more execution environments

Encryption: refers to a process of converting data or information into a code to prevent unauthorised access by human and/or computer systems.

On-premise: refers to computer systems that are located within the physical confines of Federal Public Institutions and SMEs in Nigeria.

Cloud Service Providers (CSPs): refer to local and/or international cloud computing service providers rendering service to FPIs and SMEs in Nigeria.

Cloud Consulting Service Providers (CCSP): refer to local cloud computing company or individual professional proving cloud computing consulting services to FPIs and SMEs in Nigeria.

Virtual Machine: refers to a software program or operating system that exhibits the behaviour of a separate computer and capable of performing tasks such as running applications and programs.

Vendor lock-in: refers to a situation in which FPI or SME using the cloud product or service of a cloud service provider cannot easily transition to competitor's cloud product or service.

1.0 BACKGROUND

The Nigerian Government is determined to foster the growth of the local ICT industry, significantly improve business continuity and quality of service delivery in the public sector. This policy contributes to this goal by enabling Nigerian Government (or public sector) access to cloud computing and other technologies enabled by the cloud, such as Artificial Intelligence, Machine Learning or the Internet of Things among others. This is essential for the creation of an environment that spurs development and innovation in an organic way.

Implementation of this policy will require proactive strategy to help government departments integrate cloud capabilities quickly and efficiently. This policy represents a significant step aiming to drive greater uptake of cloud services in the public sector by adopting a "cloud-first" to promote a better approach to infrastructural investments and efficient IT deployment in the public sector.

1.2 CHALLENGES

Cloud computing is a mature and stable technology and tool for commoditizing computing resources. The "cloud first" drive is aimed at addressing the challenges of acquiring and deploying IT systems in the public sector and by SMEs that provide IT-enabled services to the government. Even though IT systems of some Federal Public Institutions (FPIs) have significantly advanced individually, some are still struggling to effectively digitize their operations due to lack of resources for acquiring and deploying appropriate computing resources. On the other hand, there is no deliberate plan or incentive by the government to ease business environment for local CSPs in Nigeria. Therefore, the Nigeria Cloud Computing Policy is to address the duo categories of challenges.

The specific challenges being experienced currently by majority of public institutions and SMEs, among others are:

1. High cost of IT investments and poor sustainability of IT projects.

2. shadow IT environment that is tough to manage, difficult to operate and nearly impossible to secure;
3. Inefficient and un-scalable IT environment;
4. Poor interoperability of IT systems and inability to effectively share information and IT resources;
5. Highly competitive environment and lack of enabling business environment for local CSPs

2.0 AUTHORITY

The Nigeria Computing Cloud Policy is issued pursuant to Section 6 (a) (b) (c) and (i) of the National Information Technology Development Act 2007. The Act mandates NITDA to issue policies, frameworks, standards and guidelines for the development of IT industry in Nigeria. In view of the above, NITDA hereby issues the Policy titled "*Nigeria Cloud Computing Policy*" to promote adoption of Cloud Computing by the Government and SMEs. NITDA will work with relevant stakeholders to create enabling environment for its adoption and supervise the implementation of this policy across Federal Public Intuitions.

3.0 SCOPE OF POLICY AND ADOPTION

The Policy is applicable to all Federal Public Institutions, Public Institutions at the State and Local Government levels. The Policy shall also apply to all corporations fully or partially owned by the Federal Government in Nigeria, as data generated by these intuitions constitute data that is regarded as "Government Data".

The Nigerian Cloud Policy is issued to support government in having access to efficient IT resources that enables the public sector improve its quality of service delivery. Having access to IT resources encourages an increase in Information Technology investments.

4.0 POLICY GOAL AND OBJECTIVE

The goal of this Policy is to ensure a 30% increase in adoption of cloud computing by 2024 among Federal Public Institutions (FPIs) and SMEs that provide digital-enabled

services to the government. The policy also targets 35% growth in cloud computing investments by 2024.

In specific, the cloud computing policy is to achieve the following objectives by 2024:

1. enabling environment for the private sector to increase cloud computing infrastructure investments by 35%;
2. clear direction and programs that ensure attainment of 30% increase in cloud adoption and migration by the public sector and SMEs that provide service for the government; and
3. enabling and competitive business environment for Nigerian cloud service providers (CPS) and/or cloud consulting service providers (CCSP) to operate efficiently and profitably in the cloud market place.

This policy will also serve as useful guidance to the private sector as it continues to undertake digital transformation, the policy however acknowledges that the private sector has adopted cloud to varying degrees across sectors and therefore encouraged to continue utilizing the cloud for IT deployment.

The objectives of this policy are to develop an ongoing and iterative programme of work which will enable the use of a range of cloud services, as well as changes in the way ICT is procured and operated, throughout the Nigerian public sector. The Policy also aims to create an enabling environment for more investment in Cloud infrastructure and platforms.

Upon the publication of this policy, Nigerian public-sector entities shall prioritise the procurement of cloud-based information and communication technologies (ICTs), whenever possible. This will apply to infrastructure, hardware, software, information security, licensing, storage, and provision of data, as well as services like security, development, virtualisation, databases or any kind of technology where a cloud-based offer is essentially equivalent to other kinds of technological solutions. This will allow the Nigerian government to reduce the cost of government ICT by eliminating duplication and fragmentation and will lead by example in using cloud services to reduce costs, lift productivity and develop better services.

This policy applies regardless of whether the ICT solution under procurement is destined for end users in government service, for citizen use, or for government data centre needs.

5.0 NATIONAL CLOUD COMPUTING POLICY: KEY FACTS

The National Cloud Policy is hinged on the following facts:

i. Implementation of the country's Economic Recovery and Growth Plan (ERGP) cannot be achieved without efficient deployment of computing and digital resources. Specifically, the ERGP recognises the need to promote digital-led growth by ensuring there is increased contribution of ICT and ICT-enabled activities to GDP through significant expansion of broadband, increase in e-government and establishment of ICT clusters. Cloud computing in Public institutions and SMEs that provide service to the government can leverage cloud to enhance digital-led growth.

ii. Understanding the value that cloud computing can have in enabling efficiency, transparency, and security of public sector information and communication technology operations, in line with the spirit of the National Digital Agenda 2020, the National ICT Policy and the National Cybersecurity Strategy;

iii. The Federal Government is promoting Open Data Initiative aimed at ensuring substantial amount of public data is released for transparency purpose and creation of innovative digital services that will add value to the country socio-economic development. The best and fundamental technology to promoting Open Data is Cloud adoption.

iv. The need to lower business or market entrance barrier for SMEs by creating an enabling environment for them to safely adopt cloud computing. This ensures there is considerable reduction in capital cost due to the need to pay upfront costs for IT infrastructure including hardware, software and associated maintenance;

v. Implementation of Nigerian Government Enterprise Architecture (NGEA) at the infrastructure and security layers is largely dependent on Cloud Computing friendly environment;

vi. Recognising the need to increase the quality of the services provided by the public sector by incorporating information and communication technologies, simplifying procedures, facilitating the reengineering of processes and offering citizens the possibility of improving electronic access to personalised and coherent information and public services; and

vii. The view of NITDA (and other agencies) is that cloud computing is well suited to meet the needs of government ICT operations, from the perspective of on-demand access to computing resources, efficiency and considerably in reduction in the burden of technology management.

5.1 "Cloud First" Policy Thrust

To reap the full benefits of cloud computing, the Nigerian government is adopting this "cloud-first" policy thrust for public-sector Institutions and Government owned corporations. The cloud-first policy thrust is to also encourage adoption of cloud by SMEs to ensure they are able to provide quality, reliable and secure services to the public sector. The policy expressly articulates the government's support for cloud adoption by public-sector agencies, creating a presumption that entities shall consider cloud solutions before any other options. By this policy the government also encourages SMEs to adopt a cloud-first policy in providing service to the government.

The Policy is also designed to support the migration of government data to the cloud to drive efficiency in the operations of government and enable optimal public service delivery. It is however envisaged that pace for migration to cloud may be dictated by the availability of budgets for acquiring technology, capacity development and change management within the different agencies of Government.

NOTE: The Nigeria Cloud Computing policy provides strong consideration for Indigenous CSPs while implementing the "Cloud First" Policy Thrust except where cloud requirements or capabilities by PIs or SMEs do not exist locally.

On the other hand, the Nigeria Cloud Computing policy will ensure the cloud service provision in Nigeria is highly competitive.

5.2 Rationale for Adoption of the "Cloud First" Policy

The adoption of the cloud allows even the smallest department in the public sector to count on the same quality of IT services as a larger one. Cloud adoption is also key to saving cost and energy as hyper-scale computing is more efficient than individual servers and data centres proliferation. Government adoption of cloud services help advance clean energy goals and reduce energy consumption. This brings with it the potential to open doors to better, faster, and lower-cost services for citizens.

Among others, cloud computing could bring the following advantages to the Nigerian public-sector:

i. *Reduced Capital Cost*: Cloud computing adoption reduces initial capital cost of IT infrastructure and other computing resources as well as personnel training for public sector agencies and SMEs.

ii. *Efficiency:* Efficient technology resources can be contracted on a "pay as you use" basis and is a cost-efficient option for public sector agencies.

1. *Quality of Service and Business Continuity:* : On-demand self-provisioning characteristics of the Cloud would enhance quality of digital services and ensure there is less downtime for public service delivery.

iii. *Transparency and accountability:* It enables continuous open access to government information and data anytime and anywhere for both citizens and businesses, leading to increased engagement and participation, as well as fostering trust.

iv. *Digital Service Innovation:* Cloud computing allows for new features to be continuously deployed, while the costs are amortised across a global service customer base. New technologies such as social media, mobile platforms, and analytics tools are all available through subscriptions and enhance e-citizen services.

v. *Elasticity:* Commoditised services can grow and shrink with the level of demand; consumers pay only for what is needed to attain resources, and only for allotted time.

vi. *Information security:* Cloud-service providers hold internationally-recognised security certifications that are assessed by third-party security professionals. Cloud computing resolves information security challenges that public institutions face by providing world-class, round-the-clock monitoring and response, as well as systems designed from the ground up to only deliver data to authorised personnel and to stop attacks before they are successful. Because many cloud computing providers have advanced security features, citizen data in the cloud can be at least as, or even more secure than data in traditional on-premises solutions.

5.3 Expected Outcomes of Migration to the Cloud

The expected outcomes of Public Institutions in Nigeria migrating to the cloud include:

i. Response to public sector's need for efficient service delivery and digital transformation: Government agencies will be able to leverage services on the cloud to provide improved responsiveness to citizens' needs and increased transparency. This includes the ability to provide better healthcare, social amenities justice, public safety, and education services.

- From a public-sector perspective, the implementation of cloud services facilitates access to resources and the analysis of large data sets in order to arrive at actionable results.

ii. *Local industry development, including SMEs:* Cloud technologies will create a competitive advantage in favour of small to medium enterprises (SMEs) that drive the Nigerian economy and provide computing service to the Government.

- By adopting cloud technology, SMEs hold immense potential for generating employment opportunities, development of indigenous technology, diversification of the economic and forward-integration with established sectors such as banking, telecommunication, oil and gas among others.

iii. *Saved resources:* Migrating to the cloud can help streamline processes in many public institutions in Nigeria. Systems are too dispersed among organisations, creating inherent inefficiencies in the national public IT architecture. Instead of consolidating these services under a central government platform, which may be too rigid to meet the needs of individual organisations' applications, contracting cloud services can both drive efficiencies and enhance the customisation of IT service solutions. Also, cost savings will be expressed through:

- Finance: Government budgets are constantly scrutinised and reduced; more efficient technology resources that can be procured on a 'as needed basis;
- Time: by ensuring that the IT services have high levels of uptime and availability, and importantly, public sector agencies will not be forced to delay work due to IT outages.

iv. *Opportunities to better manage human resources:* Qualified IT professionals are a scarce resource in Nigeria and around the world. Using those resources to handle routine issues like server maintenance, patching, and other low-level support activities is wasteful of their training, experience, and talent. By moving these process-oriented tasks to cloud service providers, public institutions can invest in their human resources to re-train them for value-adding skills and activities, such as customised application development and innovative services.

6.0 CLOUD COMPUTING SERVICE AND DEPLOYMENT MODELS

The policy recognizes three basic kinds of cloud computing service offerings or cloud based service models as :

i. ***Software as a Service (SaaS):*** where the consumer uses the provider's applications running on cloud infrastructure. These applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based email) or a program interface. Fundamentally, the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples of use includes efficient tools such as accounting, email, and document management tools.

ii. ***Platform as a Service (PaaS)****:* PaaS capability is provided to consumer is a pre-installed cloud infrastructure platform such as relational database environment, Java development etc. PaaS solution provides the platform for developers to create unique, customizable software. The cloud infrastructure is consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including networking, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples include databases, programming environments, and video teleconferencing tools.

iii. ***Infrastructure as a Service (IaaS*)**: The consumer can provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly limited control of select

networking components (such as host firewalls). Examples include networking storage and virtualisation servers.

Also, the policy recognises three internationally well-known deployment models for cloud services:

ii. ***Private cloud****:* Cloud infrastructure provisioned for exclusive use by a single organisation. It is managed and operated by the organisation, a third party, or some combination of them. It may be located on- or off-premises.

iii. ***Public cloud****:* Cloud infrastructure provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider

iv. ***Hybrid cloud****:* Cloud infrastructure which is a composition of two or more distinct private and public cloud infrastructure, which remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (such as cloud bursting for load balancing between clouds).

7.0 PROCUREMENT

Government procurement is a very relevant aspect for the development of cloud computing. Traditional purchasing practices and contract terms may hinder the scalable, cost-effective, and innovative nature of cloud computing.

Agencies will consider the following factors when procuring cloud services:

i. Value for money-to fulfil the intended purpose of the service;
ii. Transitioning from capital budgets to operational expenditure;
iii. Short, medium and long terms impact on finances;
iv. The suitability of service level agreements in relation to the agency specific needs;
v. Cloud Package and subscriptions;
vi. Avoid "vendor lock in;" and

vii. Market competition.

Whereas typical procurement contracts proceed on a yearly basis, cloud service contracts are structured on a "pay as you go" basis, which permits Government to save money by paying for the services actually utilized. Furthermore, the "pay as you go" approach permits rapid scaling of services and is useful as the computing needs of an agency fluctuate. In order to ensure these are achieved, Nigerian Government will have to consider a new procurement regulation specific to cloud purchasing and services hosted in cloud environments.

NITDA will partner with the Bureau for Public Procurement (BPP) and other critical stakeholders to establish a "Digital Marketplace" which shall encompass a series of framework agreements with pre-approved cloud services suppliers and maintain a database of services in an online portal that can be accessed by procuring entities. This will guide public-sector organizations to compare and procure those services without having to do their own full review process. It will also be a way to ensure price control so as to prevent exploitation of consumers by service providers. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by NITDA and the BPP.

To be approved, cloud service providers will have to comply with the certification criteria put forward by NITDA and the BPP. Subsequent to the publication of the policy, NITDA will provide cloud computing strategy that contains guidance and framework for public institutions and SMEs on how to evaluate the benefits of cloud services and how to procure and manage them.

8.0 INTERNATIONAL DIMENSIONS OF CLOUD COMPUTING

Cloud computing brings to the forefront of the national debate several international policy issues that need to be addressed over the next years as cloud computing adoption progresses in the country. Issues to consider include:

1. Data sovereignty and Data access

NITDA will work together with government entities to find ways to strike the proper balance between local content requirements, privacy, security and intellectual property of national data. The need to identify how data is used, secured and accessed is important and therefore must be considered critically in line with relevant laws and regulations. Agencies shall consider focusing on *access to data* when required. To this end, NITDA will ensure that CSPs provide adequate security and privacy measures and transparency around data compliance.

2. Cross-Border Data Flows

To the extent that cloud information may be processed or stored in jurisdictions with privacy and information protection laws different from those in Nigeria, Agencies must do so in line with requirements of Nigerian Data Protection Regulation and any other Content Regulation. Federal Public Institutions shall be advised to contract cloud service providers that will store data in a jurisdiction that provides a level of personal data protection that is equivalent to that provided in Nigeria. NITDA will provide guidance to Federal Public Institutions to determine which jurisdictions their data may transit or be stored in.

3. Cloud computing Codes of Conduct

NITDA will work together with public-sector agencies, industry and non-governmental organisations in the development of cloud computing codes of conduct, as well as in monitoring international best practices.

9.0 DATA CLASSIFICATION

At a higher level, the issues, challenges and risks that different Public Institutions face in moving to the cloud are quite similar. Federal Public Institutions will likely have vastly different types of information and that information will contain varying levels of sensitivity. Data classification provides a tool to determine and assign relative values to the data they possess.

A simple and clear data classification framework is essential for Public Institutions as they move to the cloud. This ultimately enables individual decision makers to understand better what types of data can be stored on each type of system. This

framework also applies when considering any type of cloud either within or outside Nigeria as the cost of overprotecting the massive corpus of less sensitive data can be staggering. A robust data classification framework brings efficiencies, as it allows government entities to better align costs for bespoke security technology with highly sensitive information that requires such protection. This ensures that governments can take advantage of lower cost, commodity products or services for other less sensitive information. Thus, data classification is an essential tool that governments leverage to ensure they will be able to gain critical benefits of cloud computing in a cost-effective way.

During the construction of the framework for cloud migration, each public-sector agency shall work together with NITDA to identify the types of data the organisation has and the controls that may be required for migration to cloud services. The data is then triaged by its sensitivity, with less sensitive data generally being the primary focus of initial cloud efforts by the public-sector agency. The choice of what specific cloud solution to procure for different workloads will be linked with its classification in one of the categories described below, and thus depend on the business need and the level of security required by the agency. Data will be classified according to the following categories:

i. *Official, public or non-confidential Data (data of limited sensitivity):* This is primarily data that is publicly available and non-sensitive. It is the largest type of data held by public sector organisations and shall be immediately available for movement to cloud services. This data shall be made publicly available per the Nigeria Federal Open Data Initiative and Open Government Partnership commitments.

ii. *Confidential, routine government business data (data of moderate sensitivity):* This category may include health and financial data about natural persons. This information can be securely held in a public cloud environment if appropriate safeguards are in place. It is recommended that internal agency policies are implemented to ensure security of data. At a minimum this shall include information security awareness training for employees and contractors, and encryption of this data at rest and in motion. This type

of data must reside primarily in a cloud framework within the Nigerian territorial boundary. However, such data can be accessed, used in processing of transactions on local and international platforms for economic, developmental and policy purposes.

iii. *Secret, sensitive government and citizen data:* This type of data is related to natural and juridical persons. This data is classified as "sensitive" because the loss of confidentiality, integrity, or availability of the data could have serious, adverse, and material effects on the data subject or related entities. This data shall be moved to cloud solutions that meet the policies and legal requirements for sensitivity, including encryption of information at rest and in motion, strong user authentication, and information security awareness training all those with access to systems on which the data resides. This type of data must reside primarily in a cloud framework within the Nigerian territorial boundary. However, such data can be accessed, used in processing of transactions on local and international platforms for economic, developmental and policy purposes.

iv. *Classified or National security information:* This type of data is considered sensitive to national security and thus requires additional safeguards. Security Services and NITDA will review data deemed national security sensitive to determine the options for this data type. Exceptions to this policy can be made for data that NITDA and the public institutions certify are related to legitimate national security concerns. This type of data can and shall be moved to the cloud, but requires solutions deemed appropriate for national security information, including private cloud options. This type of data must reside only on-premise of the public institutions or collocated or in a cloud within the Nigerian territorial boundary.

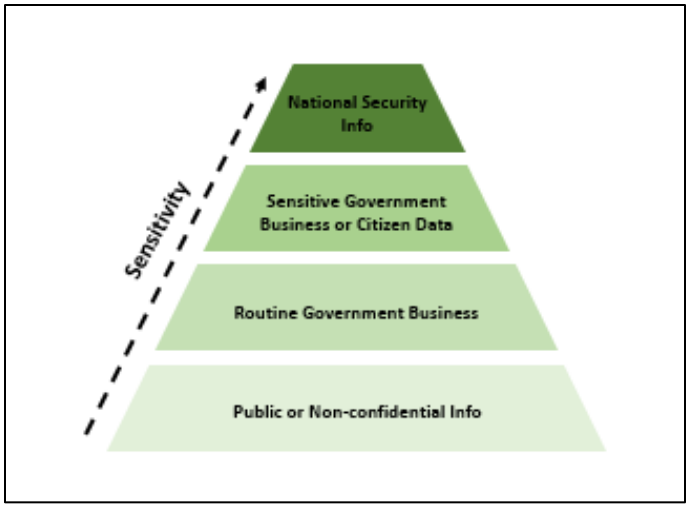

Figure 1: Data classification

10.0 INFORMATION SECURITY

Data classification is often designed hand-in-hand with information security requirements that are appropriate for managing each level of information. Information security refers to the protection of information systems against unauthorised access, use, disclosure, disruption, modification or destruction, primarily by third parties. It is a cloud service provider's (CSP) obligation to protect its cloud system and the confidentiality, integrity and availability of its data. A (cloud services) customer, including all Public Institutions shall make use of cloud services and select the information security level which best matches their specific needs and security requirements, and to inform CSPs accordingly. Data classification requirements may be set out in the internal rules for a government agency or will be applicable by legislation, regulations, policy or administrative instructions.

Using the same Data Classification framework provided above, for security purposes, data is classified into 3 levels depending on their level of sensitivity (from 1- least sensitive, to 3- more sensitive). The higher the level of security, the stricter the information security requirements for the CSP, such as strong encryption mechanisms, backups etc.

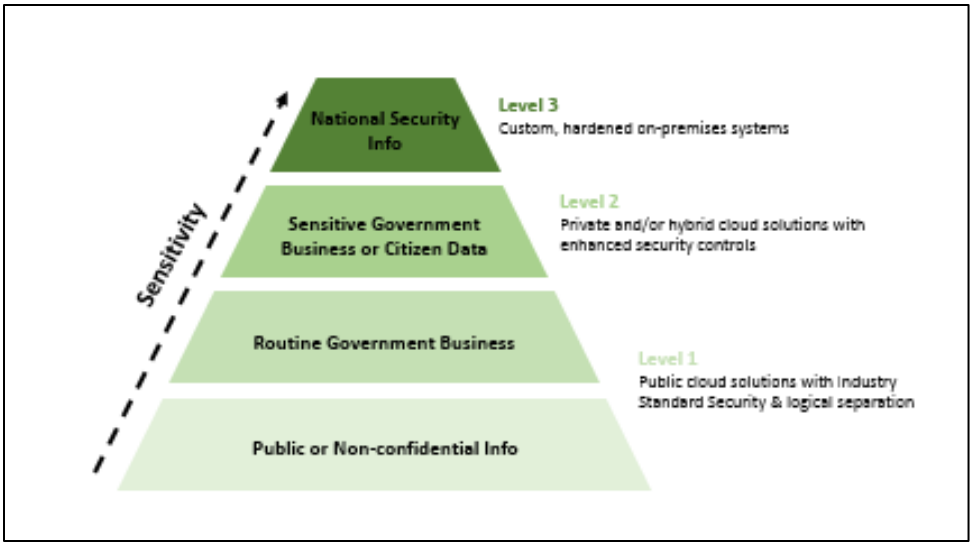

Figure 2: Information security levels

In light of the updated data classification framework, agencies will have to reconsider the sensitivity of the data and if it still requires that government data be kept only within the Nigerian territory. It is up to the government agencies concerned to ensure that their use of any Cloud services remains compliant with any such applicable rules, in addition to those set out in the Regulatory Framework. CSPs do not have the access or capability to monitor their customers' data and content, maintaining a strict adherence to the level of confidentiality that government agencies require.

Government departments are encouraged to seek further guidance from NITDA. NITDA will retain these frameworks and is empowered to begin consolidating the experiences of various public-sector organisations into best practices on topics including but not limited to: data migration, contract negotiation, service level agreements, and budget management.

11.0 INTEROPERABILITY REQUIREMENTS

Public Institutions shall require interoperability of the components of a cloud infrastructure to work together to achieve the intended result based on national interoperability framework such Nigerian e-Government Interoperability Framework (Ne-GIF) and international standards, such as ISO/IEC 17203:2011. The components may come from different sources including public and private cloud implementations.

The components shall be replaceable by new or different components from different cloud service providers (CSPs) and continue to work, to facilitate the exchange of data between systems.

12.0 CONSUMER PROTECTION

NITDA will work on the development of a regulatory framework for the execution of cloud computing contracts between Public Institutions and Cloud Service Providers (CSP). This regulatory framework shall ensure that government entities using the cloud as cloud customers enjoy at least the same rights as those enjoyed by individual customers, enterprises and other cloud customers.

Among others, the regulatory framework will provide an inclusion in the contracts for government entities of minimum requirements, such as:

i. CSP adherence to the due diligence process and conformity of public procurement guidelines/processes;
ii. a description of services to be provided;
iii. the contract's duration (unless it is of unlimited duration);
iv. payment terms and termination;
v. details on the available Service Level Agreements (SLA);
vi. rules on handling cloud customer data, including their processing, destruction and restoration;
vii. CSP's customer care services depending on a particular service offering;
viii. customers' right to retrieve their data stored in the CSP's system, if the cloud contract is terminated; and
ix. limitation of CSPs' right to exclude their liability unreasonably or to impose unfair contract terms related, for instance, to any loss of, or damage to, customer's data, quality of service degradations such as service unavailability, or data breaches.
x. Level of cloud security and privacy.

13.0 SERVICE LEVEL AGREEMENTS (SLAS)

Service Level Agreements (SLAs) are undertakings that are binding for the service provider on the service level. Among other things, they stipulate penalties for the service provider if the contractual undertakings are not fulfilled. They are particularly important with regards to clauses on data protection (retention period, exercise of rights of data subjects, availability of processing, etc.).

The provisioning of cloud computing by cloud service providers (CSPs) to government entities shall be governed by SLAs to specify and clarify performance expectations and establish accountability. The SLAs shall relate to the provisions in the contract regarding incentives, penalties, escalation procedures, disaster recovery and business continuity, and contract cancellation for the protection of the government entity in the event the CSP failed to meet the required level of performance.

Government entities shall closely monitor the CSP's compliance with key SLA provision on the following aspects, among others:

i. availability and timeliness of services;
ii. confidentiality and integrity of data;
iii. change control;
iv. security standards compliance, including vulnerability and penetration management;
v. business continuity including disaster recovery and contingency plans; and
vi. Help Desk Support

14.0 MIGRATION TO THE CLOUD

The broad scope and size of the cloud transformation will require a meaningful shift in how Nigerian public-sector entities think of IT. Those that previously thought of IT as an investment in on premise applications, servers, and networks will now need to think of IT in terms of services, commoditised computing resources, aimed at making computing resources accessible on demand and at a reasonable cost with quality of

service guaranteed based on the provisions in the cloud service SLA. This new way of thinking will have a broad impact across the entire IT service lifecycle – from planning to delivery and operations.

This policy is to be effective upon publication but a 12-month grace period, or at the earliest, will be permitted for compliance. Thereafter, a recommended gradual migration up to one year will take effect which requires each public-sector agency to develop an implementation plan in line with national framework for cloud migration. The migration plan will prioritize new IT systems to replace legacy systems. In due time, NITDA will provide strategy for government agencies on the phases and preparation for migration.

The following structured framework provides a strategic perspective for public-sector entities to plan for cloud migration:

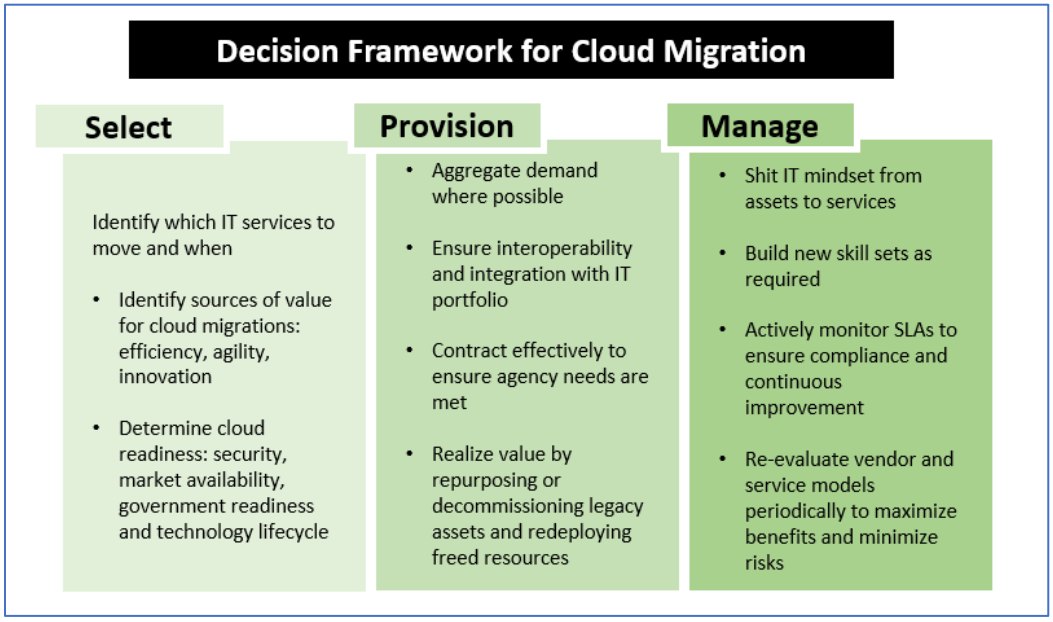

Figure 3: Cloud Migration Decision framework

Public Institutions shall carefully consider their broad IT portfolios and create roadmaps for cloud deployment and migration. These roadmaps shall prioritise services that have high expected value and high readiness to maximise the benefits received and minimise the delivery risk. Agencies are expected to produce a road map which will help to determine which skills to retrain among their IT-professionals in order to mitigate cloud migration risks. The road map will further define exactly

which cloud services an entity intends to provide or consume as an essential initiation phase of the road map.

15.0 AUDITS

NITDA, directly or through each individual public-sector agency contracting with a cloud service provider (CSP), may require a CSP to provide satisfactory audit reports or respond to audit requests. This is meant to ensure that data centre facilities provide adequate levels of protection for the treatment of public sector information assets (as determined by their classification under the Data Classification Framework)**.** NITDA, and certified third-parties will be able to monitor and perform audits to validate the contractually agreed controls. Unless otherwise indicated, the audits will occur yearly.

16.0 CLOUD CERTIFICATIONS

Cloud service providers (CSPs) servicing Public Institutions must be compliant with the cloud security certification programs that the Nigerian government will establish.

Security certification programs provide visibility and transparency in CSPs' security practices. This visibility is achieved through an audit or assessment that a professional third-party assessment organisation conducts against a security-control framework. Consumers of the service – such as Public Institutions– can then leverage these certifications to ensure key security requirements are being met. Among others, these include:

i. International Standards Organisation ISO 27001

ii. Code of practice for cloud privacy ISO/IEC 27018

17.0 WORKFORCE AND SKILLS

The adoption rate of cloud services is directly correlated to the rate at which IT professionals can acquire cloud skills. It is essential that Nigerian Government articulates how the transition to the cloud could change the labour requirements for

FPIs, and how labour resources might be reallocated to enable them provide more value to its stakeholders and further add value to the Nigerian information technology labour pool.

Successful cloud adoption in the Nigerian public sector will depend on developing talent and acquiring professional IT credentials. NITDA will work on the formulation and implementation of the necessary policies for training human resource individuals in cloud computing. These policies shall focus on ensuring IT professionals can develop enhanced skills and competencies in the following areas among others:

i. business acumen, to better understand the services and expectations of business partners in their departments and across government as a whole;

ii. analytical capacity, to evaluate the various options for delivering IT services, based on a broad range of criteria;

iii. vendor-management relations, for example, evaluate, negotiate, monitor and enforce contracts, SLAs, to ensure that the government receives full value for its funding and full benefits under the contracts or arrangements; and

iv. new technology adapted to emerging areas such as architecture and deployment of solutions to the cloud.

For the adoption of cloud to be successful, the Nigerian Government must immerse itself in a cloud ecosystem, surrounding itself with both skilled employees and experienced professional services. Chief Information Officers (CIOs) within the Nigerian Government must understand the changing environment, undertake the necessary workforce planning, and invest in their workforce in order to provide their IT professionals with the necessary learning and developmental opportunities.

Furthermore, cloud computing is a wide-reaching IT initiative. Impacts will be great and widespread in the following areas: application development; IT operations; legal services; finance; procurement; security; compliance; privacy; identity management; data integration; mobility; and customer service. Director/Head of ICT/IT in Federal Public Institutions are encouraged to appoint a cloud leader to direct a cloud core team to address organisational transformation.

18.0 VENDOR LOCK-IN

Cloud customers may decide to change between CSPs for a variety of reasons. It is important that their initial migration to the cloud avoids vendor lock-in and facilitates future migration between platforms. Public sector organizations can insure against vendor lock-in by ensuring cloud technologies acquisition follows open standards definitions and as well follow the Nigeria e-Government Interoperability Framework (Ne-GIF) specifications in their procurement processes. If public sector organizations build their infrastructure based on the Open Virtualization Format (OVF) and Cloud Data Management Interface (CDMI), this will facilitate migration of data to the cloud and between CSPs. Organizations shall consider the necessity of migrating potentially large quantities of data to launch a service, and the ability to increase data scale if ever it becomes necessary.

19.0 DATA WITHDRAWAL

Organizations shall consider how any data within the system can be retrieved and returned when the contract for cloud services expires. They shall ensure that the cloud provider specifies how data will be transferred back if required and agree on timeline, which shall be included within the contract. Most importantly, all government agencies shall instruct copies of the data to be deleted, overwritten or otherwise rendered inaccessible upon expiration or termination of a contract.

20.0 NATIONAL CLOUD COMPUTING GOVERNANCE

This cloud-first policy is the first step in the process of migrating towards cloud technologies within the Nigerian public sector. Cloud computing governance is a view of IT governance focused on accountability, defining decision rights, and balancing benefit or value, risk, and resources in a cloud computing friendly environment. The purpose of implementing a solid governance framework is that it ensures expenditures related to cloud are aligned with an agency's objectives, promote data integrity across the agency, encourage innovation, and mitigate the risk of data loss or non-compliance with regulations. It also recognizes that cloud computing increases the pervasive nature of IT and ensures decision-makers are able to effectively

manage overall IT investment, resource requirements, opportunities for value, and implications of risk – regardless of organization or delivery provider. Agencies will be responsible for evaluating their sourcing strategies to fully consider cloud computing solutions.

The plan shall operate across four levels of cloud governance:

i. the infrastructure, or virtualization platform
ii. the operating system
iii. the platform or application
iv. the business/user activity on that platform

It shall consider four operations categories at each of those levels:

i. application deployment and lifecycle
ii. security and privacy
iii. management and monitoring
iv. operations and support

The following bodies shall have these roles and responsibilities:

i. Bureau of Public Procurement shall develop and operationalize government-wide procurement regulation for Cloud services in consultation with NITDA and other relevant agencies of government;
ii. NITDA will liaise with the BPP to accommodate cloud procurement models in the procurement process;
iii. NITDA shall conduct a Cloud readiness assessment;
iv. The Office for National Security Adviser (ONSA) and NITDA shall monitor operational security issues related to the cloud;
v. NITDA shall drive government-wide adoption of cloud, identify next-generation cloud technologies, share best practices, templates and reusable example;
vi. NITDA shall coordinate activities across governance bodies, set overall cloud-related priorities, and provide guidance to agencies; and

vii. NITDA shall monitor, identify and prioritize cloud computing standards and guidance from the National Institute of Standards and Technology (NIST), International Organisatiom for Standardization (ISO) and other relevant international standards organisations.

To effectively manage these governance issues in the long-term, NITDA will seek to lay a stable governance foundation that will outlast single individuals or administrations. Individuals or committees will have explicitly defined roles, non-overlapping responsibilities, and a clear decision-making hierarchy. These steps will empower the government for action, minimise unnecessary bureaucracy, and ensure accountability for results.

21.0 ENFORCEMENT PROCEDURES

As a general rule of thumb, the CSP shall maintain the utmost integrity to protect the data and meet the security requirements set forth my NITDA. Data shall not be stored, shared, processed, or modified by in any way that compromises the integrity of the data. The failure to satisfy any of the liabilities or obligations on the part of the CSP shall constitute a breach of the contract. Violation of the contract or breach of data shall be disclosed by the CSP to NITDA as soon as the breach is discovered. NITDA or a directed organization identified by NITDA will conduct a root cause analysis and determine appropriate sanctions. NITDA shall issue guidelines for compliance and enforcement of this policy in the cloud computing implementation framework and strategy.

22.0 KEY REGULATORY INSTRUMENTS FOR THE ACTUALIZATION OF CLOUD POLICY

The implementation of cloud computing will require among others, the development and operation of a cloud computing strategy, compliance framework and regulations that include the following:

i. Cloud Infrastructure Standards Regulation

ii. Digital Services Marketplace and Procurement Guidelines

iii. Framework for Cloud Adoption and Migration

iv. Cloud Computing Code of Conduct

v. Compliance and Enforcement Framework

23.0 PROGRAMS FOR CLOUD COMPUTING IMPLEMENTATION

The following programs among others, will be carried out to implement the policy:

i. Cloud Computing readiness assessment;
ii. Cloud Computing adoption and promotion for public sector organizations;
iii. Cloud Computing adoption and promotion for SMEs;
iv. Promotion of enabling environment for increased cloud computing investment in Nigeria;
v. Cloud Computing Service providers and consulting firms' certification;
vi. Setting and operationalizing cloud computing governance structure; and
vii. Capacity and capability programs for cloud computing;
viii. Baseline study and partnerships with all sectors of the economy;
ix. Local content for Nigerian Cloud Service Providers

24.0 EFFECTIVE DATE

This policy shall take effect upon its publication. After that, it will be subject to a bi-annual review or as the need arises. NITDA shall issue further guidance on the evaluation process and timeframe to make changes and updates.

THIS POLICY IS HEREBY ISSUED ON THE 2ND DAY OF AUGUST, 2019

BY THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA)

…..……

Dr Isa Ali Ibrahim (Pantami) PhD, FNCS, FBCS, FIIM
Director General/ CEO
Chief Information Technology of Nigeria.