National Cloud Computing Policy

National Information Technology Development Agency

(NITDA)

2019

Content

National Cloud Computing Policy

1.0 BACKGROUND

The benefits of cloud computing adoption by Nigerian Government and her Ministries, Departments, Agencies and Institutions could lead to capital costs reduction, improved responsiveness to citizens' or customers' needs, increased transparency and enhanced public service delivery. In addition, cloud computing adoption could also facilitate creation of new jobs and help Small Medium Enterprise (SMEs) cross the barrier of initial IT capital and investment challenges. However, cloud computing fundamentally changes how organisations use IT and introduces challenges and risks that need to be managed to ensure that they take full advantage of the potential of this technology.

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

Moving forward requires a proactive strategy to help government departments integrate cloud capabilities quickly and efficiently. The policy represents a significant step in this direction, aiming to drive greater uptake of cloud services in the public sector by adopting a cloud-first approach

Therefore, the National Information Technology Development Agency (NITDA) provides cloud computing policy as a guidance to help public sector and SMEs manage cloud adoption and ensure they get a fair deal from cloud service providers.

It is also expected that the policy to be relevant for organisations in a variety of sectors. Specifically, the Nigerian Government is determined to foster the growth of the local ICT industry. This policy contributes to this goal by enabling Nigerian Government (or public sector) access to cloud and other technologies enabled by cloud, such as Artificial Intelligence, Machine Learning or the Internet of Things. This is essential for the creation of an environment that spurs development and innovation in an organic way.

Moving forward requires a proactive strategy to help government departments integrate cloud capabilities quickly and efficiently. The policy represents a significant step in this direction, aiming to drive greater uptake of cloud services in the public sector by adopting a cloud-first approach.

2.0 AUTHORITY

The Nigerian 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 "*National 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 TYPES OF CLOUD COMPUTING AND DEPLOYMENT MODELS

National Institute of Standards Technology (NIST) defines Cloud Computing as 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.

The followings are the three kinds of computing service offerings or cloud based service models:

- ***Software as a Service (SaaS):*** The consumer can use the provider's applications running on cloud infrastructure. The 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. 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 include accounting, email, and document management tools.

- ***Platform as a Service (PaaS)****:* The capability provided to consumer is a pre-installed cloud infrastructure platform such as relational database environment, Java development etc. A 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.
- ***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.

There are three internationally recognised deployment models for cloud services:

- ***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.

- ***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
- ***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).

4.0 NIGERIAN CLOUD FIRST POLICY

The Nigerian Cloud First Policy is hinged on the following facts:

I. 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;

II. As the Nigeria Federal Open Data Initiative aims to promote the creation of value for all stakeholders in the publication of government data for innovative uses;

III. 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;

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

V. 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

VI. 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 less burden of technology management.

4.1 Cloud First Policy

To reap the full benefits of cloud computing, the Nigerian government is adopting this cloud-first policy for public-sector Institutions, Government owned corporations. The cloud-first policy is to also encourage adoption of cloud by SMEs. 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 data storage options. The government is to also support SMEs and encourage them to adopt cloud-first policy.

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 to availability of budgets for acquiring technology, capacity development and change management within the different tiers of Government.

4.2 Rationale for Adoption of "Cloud First" Policy

The adoption of the cloud allows even the smallest agency in with 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 proliferation data centres. 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:

- *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. Especially, those ones that are
- *Efficient (cost of) governance:* Efficient technology resources can be contracted on a “pay as you use” basis and is a cost-efficient option for public sector agencies. Likewise, it enables open access to (non-sensitive) government information and data for both citizens and businesses, leading to increased engagement and participation, as well as fostering trust.
-
- *Transparency and accountability:* It enables 24 hours open access to government information and data for both citizens and businesses, leading to increased engagement and participation, as well as fostering trust.
- *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.
- *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.
- *Data privacy:* 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.
- *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.

4.3 Expected Outcomes of Migration to the Cloud

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

- *Response to public sector's need for 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, 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.
- *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.
- *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;
  - Personnel: allowing the country's high-demand IT professionals to focus on larger, more strategic issues, an overall benefit to the country; and
  - 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.

- *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.

5.0 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, in so far as data generated by these intuitions constitute data that may be 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 increased in Information Technology investments.

6.0 POLICY GOAL AND OBJECTIVE

The goal of this Policy is to ensure adoption of various cloud computing models by Federal public institutions reaches 30% by the end of 2024. Also, the policy is to create an enabling environment for 30% adoption of cloud by SMEs and 35% growth in cloud computing investments by private sector at the end of 2024The goal of

In specific, by the end of 2024, the objectives of cloud policy are to:

1. promote increased investment and adoption in cloud computing infrastructure in Nigeria;
2. set direction and outline programs that ensure attainment of 30% adoption and migration to the cloud by public sector;Promote increased investment and adoption in cloud computing infrastructure in Nigeria;
3. set direction and outline programs that ensure attainment of 30% adoption of Cloud Computing by SMEs;
4. create enabling business environment for cloud computing service providers and consulting services; and
5. promote increased investment in cloud computing infrastructure

The goal of this policy is to guide government agencies in the transition to cloud computing to improve accessibility, quality, efficiency, security, and reduce cost of government services. This policy will also serve as useful guidance to the private sector as it continues to undertake digital transformation, but the private sector is not obliged to comply.

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.

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.

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:

- Value for money-to fulfil the intended purpose of the service;
- Transitioning from capital budgets to operational expenditure;
- Short, medium and long terms impact on finances;
- The suitability of service level agreements in relation to the agency specific needs;
- Avoid “vendor lock in;” and
- 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 operation.

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. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by NITDA and the BPP.

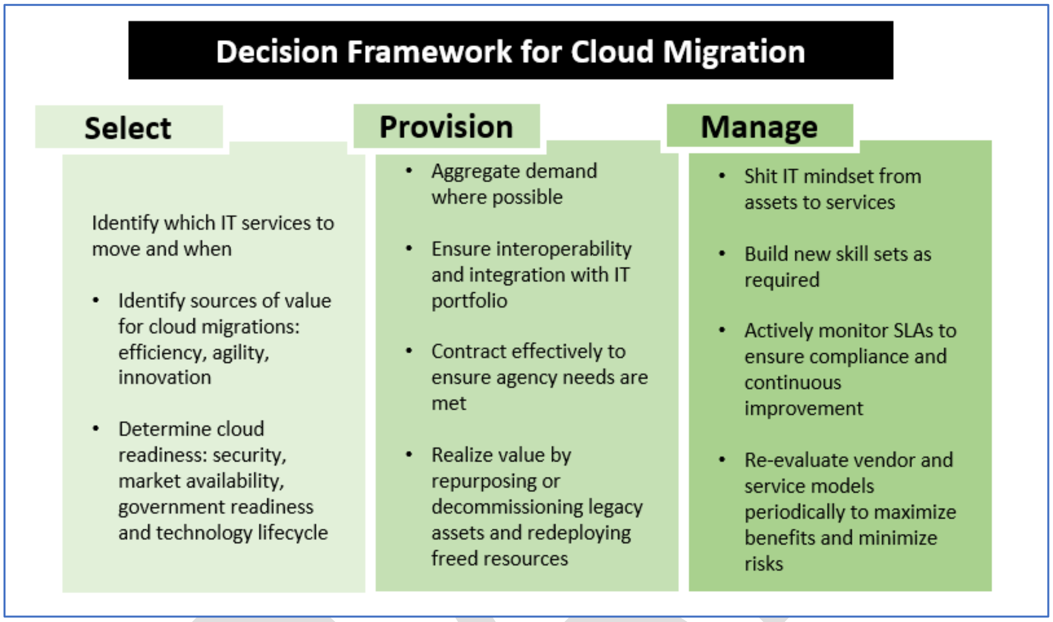
To be approved, cloud service providers will have to comply with the certification criteria put forward by NITDA and the BPP. Subsequent to the publication of the policy, NITDA will provide cloud computing strategy that contains guidance and framework for public institutions and SMEs on how to evaluate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

8.0 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, agile capacity and computing provisioning tools, and their enabling effect on Nigerian citizens. 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:



Decision Framework for Cloud Migration

Select

Identify which IT services to move and when

- Identify sources of value for cloud migrations: efficiency, agility, innovation
- Determine cloud readiness: security, market availability, government readiness and technology lifecycle

Provision

- Aggregate demand where possible
- Ensure interoperability and integration with IT portfolio
- Contract effectively to ensure agency needs are met
- Realize value by repurposing or decommissioning legacy assets and redeploying freed resources

Manage

- Shit IT mindset from assets to services
- Build new skill sets as required
- Actively monitor SLAs to ensure compliance and continuous improvement
- Re-evaluate vendor and service models periodically to maximize benefits and minimize risks

Figure 1: 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. Defining exactly which cloud services an entity intends to provide or consume is an essential initiation phase activity in developing an agency roadmap.

9.0 INTERNATIONAL DIMENSIONS OF CLOUD COMPTUING

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. MDAs 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 MDAs 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.

10.0 DATA CLASSIFICATION

At a higher level, the issues, challenges and risks that different Public Institutions face in moving to the cloud are quite similar. That said, MDAs 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:

- *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.
- *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.

- *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.
- *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 on-premise of the public institutions or collocated or in a cloud within the Nigerian territorial boundary.

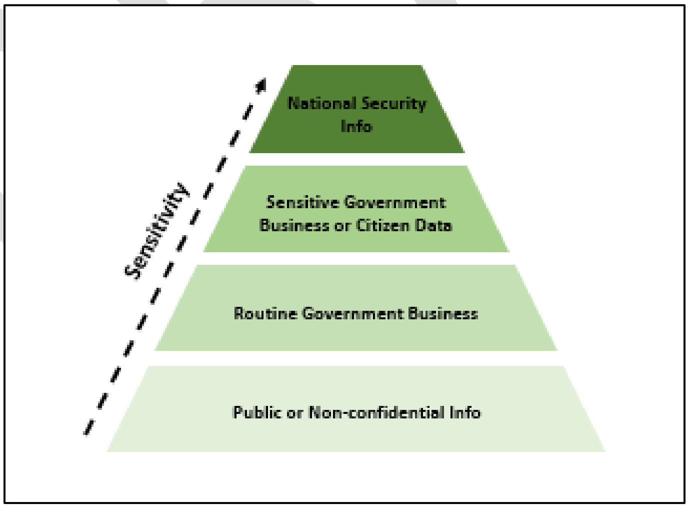

National Security Info
Sensitive Government Business or Citizen Data
Routine Government Business
Public or Non-confidential Info
Sensitivity

Figure 2: Data classification

11.0 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.

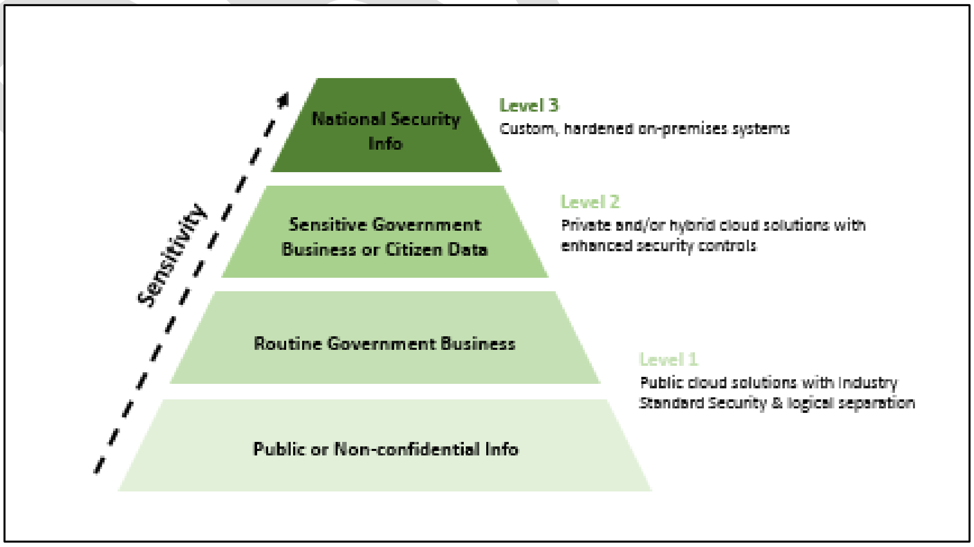

Sensitivity
National Security Info
Sensitive Government Business or Citizen Data
Routine Government Business
Public or Non-confidential Info
Level 3
Custom, hardened on-premises systems
Level 2
Private and/or hybrid cloud solutions with enhanced security controls
Level 1
Public cloud solutions with Industry Standard Security & logical separation

Figure 3: 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 inside 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 hereby empowered and requested 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.

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:

- CSP adherence to the due diligence process and conformity of public procurement guidelines/processes;
- a description of services to be provided;
- the contract's duration (unless it is of unlimited duration);
- payment terms and termination;
- details on the available Service Level Agreements (SLA);
- rules on handling cloud customer data, including their processing, destruction and restoration;
- CSP's customer care services depending on a particular service offering;

- customers’ right to retrieve their data stored in the CSP’s system, if the cloud contract is terminated; and
- 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.

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:

- availability and timeliness of services;
- confidentiality and integrity of data;
- change control;
- security standards compliance, including vulnerability and penetration management;
- business continuity including disaster recovery and contingency plans; and
- Help Desk Support

14.0 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 may not be stored, shared, processed, or modified 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.

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 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.

17.0 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:

- International Standards Organisation ISO 27001
- Code of practice for cloud privacy ISO/IEC 27018

18.0 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 the agency, and how labour resources might be reallocated to enable the agency to 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 areas such as:

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

- analytical capacity, to evaluate the various options for delivering IT services, based on a broad range of criteria;
- 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
- 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 MDAs are encouraged to appoint a cloud leader to direct a cloud core team to address organisational transformation.

19.0 LOCK-IN AND MIGRATION

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 defining technology standards and following the Nigerian Government Enterprise Architecture (NGEA) especially the infrastructure layer of the reference models in their procurement processes. If public sector organizations build their infrastructure using standard and widely available components such as virtual machines (VMs), 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.

20.0 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.

21.0 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 an environment embracing cloud computing. 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 address the 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:

a. the infrastructure, or virtualization platform
b. the operating system
c. the platform or application

d. the business/user activity on that platform

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

e. application deployment and lifecycle
f. security and privacy
g. management and monitoring
h. operations and support

The following bodies shall have these roles and responsibilities:

- Bureau of Public Procurement shall develop and operationalize government-wide procurement regulation for Cloud services procurement in consultation with NITDA and other relevant agencies of government
- the Office for National Security Adviser (ONSA) and NITDA shall monitor operational security issues related to the cloud.
- NITDA shall drive government-wide adoption of cloud, identify next-generation cloud technologies, and share best practices and reusable example analyses and templates.
- NITDA shall coordinate activities across governance bodies, set overall cloud-related priorities, and provide guidance to agencies.
- Also, NITDA shall monitor, identify and prioritize cloud computing standards and guidance from the National Institute of Standards and Technology (NIST).

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.

21.1 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. Data Classification Framework

V. Cloud Computing Code of Conduct

VI. Compliance and enforcement framework

22.0 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

23.0 EFFECTIVE DATE

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

[signature, date, public registration]