NATIONAL GUIDELINE FOR CLOUD COMPUTING IN NIGERIA 2026

Document Information

S/N	Data Element	Value
1	Title	National Cloud Computing Guideline 2026
2	Short Title	National Cloud Computing Guideline
3	Document Identifier	
4	Version	Version 1.0
5	Approval Date	4th August 2026
6	Effective Date	1st January 2027
7	Publisher	National Information Technology Development Agency (NITDA)
8	Document Type	Guideline
9	Enforcement Status	Mandatory
10	Document Owner	National Information Technology Development Agency (NITDA)
11	Custodian	Regulations & Compliance Department
12	Target Audience	Federal Public Institutions (FPIs); State Governments; Local Governments; Cloud Service Providers; Data Centre Operators; ICT Service Providers; Service Integrators; Professional Bodies; Development Partners; and other organisations within the scope of this Guideline.
13	Legal Authority	NITDA Act, 2007 and other applicable laws, regulations and government policies.
14	Related Documents	National Sovereign Cloud Policy; National Data Classification & Localisation Framework; National Cloud Technical Guideline; National Digital Infrastructure Assurance Framework.
15	Review Cycle	Every three (3) years or as required.
16	Language	English
17	Format	Electronic (PDF)
18	Subject	Cloud Computing, Cloud Governance and Cloud Adoption
19	Classification	Public
20	Copyright	

Table of Contents

Interpretation

1. Status of Schedules

The Schedules (A - D) form an integral part of this Guideline and have the same binding legal effect as the main body. Compliance with one Schedule does not exempt any FPI, CSP, or SI from obligations under any other Schedule or under applicable laws (including the NDPA 2023 and the Public Procurement Act, 2007).

2. References to Laws and Regulations

References to any Act, Regulation, Executive Order, or statutory instrument shall be deemed to include any amendments, consolidations, or re-enactments thereof, unless expressly stated otherwise.

3. Definitions Control

Capitalised terms used in this Guideline shall have the meanings assigned to them in the Glossary unless the context otherwise requires. Where a term is defined in both this Guideline and in another applicable law (such as the NDPA 2023), the definition under the applicable law shall prevail.

4. Headings and Numbering

Headings, sub-headings, numbering, and formatting in this Guideline are for convenience only and do not affect interpretation.

5. Conflict of Provisions

In the event of any conflict:

(a) The provisions of Nigerian law (including the NITDA Act 2007, NDPA 2023, Public Procurement Act 2007, and Cybercrimes (Amendment) Act 2024) shall prevail over this Guideline;

(b) This Guideline and its Schedules shall prevail over any conflicting internal policy, contract, or practice of an FPI, CSP, or SI, unless expressly exempted by NITDA;

6. Use of "Shall", "Must", "May"

(a) "Shall" and "Must" indicate mandatory obligations.

(b) "May" indicates discretionary or permissive action.

(c) "Should" indicates recommended best practice which, while not legally mandatory, is expected to be followed unless a documented justification exists.

7. Singular and Plural

Words importing the singular include the plural and vice versa.

8. Persons

References to "persons" include legal entities (corporate or unincorporated), statutory bodies, partnerships, and associations, unless the context otherwise requires.

9. Time Periods

Any reference to a number of days shall be interpreted as calendar days unless expressly stated as "working days".

1 This Guideline shall be described as '**National Cloud Computing Guideline, 2026**'. **Long Title**

2 This Guideline may also be cited as "**National Cloud Computing Guideline**". **Short Title**

3 The Federal Government of Nigeria, through the National Information Technology Development Agency (NITDA), issues the National Cloud Computing Guideline 2026 (NCG2026) to establish a secure, resilient, sovereign, and investment-friendly cloud ecosystem that supports Nigeria's digital transformation and strengthens the country's digital economy. **Explanatory Note**

The Guideline establishes the national governance framework for cloud adoption, cloud services, and supporting digital infrastructure in Nigeria. It promotes a Cloud First approach for Federal Public Institutions (FPIs) while prescribing nationally recognised principles, governance requirements, and minimum standards applicable to Cloud Service Providers (CSPs), Service Integrators (SIs), Data Centre Operators, Artificial Intelligence Infrastructure Providers, and other Digital Infrastructure Providers operating within Nigeria.

The Guideline provides a unified framework for cloud governance by establishing requirements for data classification, data sovereignty, cloud security, operational resilience, interoperability, risk management, indigenous participation, and investment promotion. It further seeks to strengthen trust in Nigeria's cloud ecosystem by supporting internationally recognised standards, encouraging innovation, promoting fair competition, and creating an enabling environment for sustainable investment in cloud and digital infrastructure.

The Guideline is complemented by the National Cloud Technical Guideline, the National Cloud Investment Strategy, and the National Digital Infrastructure Assurance Framework (NDIAF), which collectively

provide the technical standards, investment framework, certification, and assurance mechanisms necessary to support trusted cloud adoption across government, regulated sectors, and the wider digital economy.

To facilitate effective implementation, NITDA may issue additional frameworks, implementation guidelines, codes of practice, operational manuals, certification schemes, technical specifications, advisories, and other regulatory instruments from time to time. These instruments may address specific aspects of cloud computing, digital infrastructure assurance, sovereign cloud, artificial intelligence infrastructure, digital marketplaces, interoperability, cybersecurity, operational resilience, and other emerging technologies or implementation requirements.

Through these instruments, NITDA seeks to position Nigeria as a leading regional hub for cloud computing, sovereign digital infrastructure, artificial intelligence, and data-driven innovation while ensuring that cloud adoption contributes to national security, economic growth, digital sovereignty, and the long-term development of Nigeria's digital ecosystem.

4 **Authority**

In the exercise of the mandate conferred on it by Section 6 of the National Information Technology Development Agency Act, 2007, the National Information Technology Development Agency (NITDA), in compliance with the provisions of Section 32 of the NITDA Act, hereby issues the "**National Cloud Computing Guideline, 2026**".

5 **Commencement**

The Guideline shall come into effect on 1st January 2027.

6 **Application and Scope**

This Guideline establishes Nigeria's national framework for the adoption, procurement, deployment, operation, management, and assurance of cloud computing services and supporting digital infrastructure. It governs the acquisition and use of cloud services by Federal Public Institutions (FPIs) and prescribes the minimum standards, governance, security, operational, and

assurance requirements applicable to Cloud Service Providers (CSPs), Service Integrators (SIs), Data Centre Operators, Managed Service Providers, Artificial Intelligence Infrastructure Providers, and other Digital Infrastructure Providers operating or providing cloud-related services within Nigeria.

This Guideline shall apply to new cloud deployments as well as existing implementations. Existing deployments within its scope shall be reviewed and brought into compliance within a transition period prescribed by NITDA through implementation guidance.

6.1 Entities Covered

This Guideline and its associated schedules, technical guidelines, and supporting instruments shall apply to the following:

I. Federal Public Institutions (FPIs)

This Guideline is mandatory for all Federal Public Institutions, Federal Government-owned companies, and any other entities designated by the Federal Government. Such institutions shall comply with the Cloud First Principle and all applicable procurement, governance, security, and operational requirements prescribed under this Guideline.

II. Cloud and Digital Infrastructure Providers

This Guideline is mandatory for Cloud Service Providers (CSPs), Service Integrators (SIs), Data Centre Operators, Managed Service Providers, Artificial Intelligence Infrastructure Providers, Sovereign Compute Providers, and other Digital Infrastructure Providers operating within Nigeria or providing cloud and digital infrastructure services to entities within the scope of this Guideline. Such providers shall comply with the applicable technical, security, assurance, certification, and operational requirements prescribed by NITDA.

III. Contractors, Partners, and Outsourcing Providers

This Guideline shall apply to contractors, concessionaires, Public-Private Partnership (PPP) operators, outsourcing providers, managed service providers, payment processors, technology vendors, and any other entities processing, storing, transmitting, managing, or supporting government information or digital services on behalf of Federal Public Institutions. Compliance shall be incorporated into contractual arrangements and shall extend to subcontractors, sub-processors, and other downstream service providers engaged in the delivery of such services.

IV. State Governments and Other Public Institutions

State Governments, Local Governments, and other public institutions are encouraged to adopt this Guideline to promote a harmonised national cloud ecosystem, strengthen interoperability, and facilitate secure data sharing across all tiers of government.
State participation shall be facilitated through the subnational opt-in arrangements of the National Sovereign Cloud Policy, including access to negotiated rates and capacity secured under federal anchor arrangements.

V. Regulated Sectors and Nationally Significant Data

The data governance, security, data residency, operational resilience, and assurance requirements of this Guideline shall apply to providers supporting regulated sectors and to organisations processing, storing, transmitting, or managing data designated by NITDA, the Office of the National Security Adviser (ONSA), or the relevant sector regulator as being of strategic national importance. Nothing in this Guideline shall prejudice or limit the statutory powers or sector-specific regulatory requirements of competent authorities.

7 The primary goal of this Guideline is to achieve a minimum of seventy-five percent (75%) adoption of cloud-based services across Federal Public Institutions (FPIs) by 31 December 2030, and to stimulate sustained year-on-year growth of not less than thirty-five percent (35%) in national cloud computing investments within the same period. **Objectives**

Specific objectives include:

I. To promote a secure, resilient, interoperable, and trusted national cloud ecosystem that supports government, businesses, critical information infrastructure, digital public infrastructure, financial system resilience, and the wider digital economy.
II. To stimulate the development and consumption of high-quality digital products and services from indigenous companies.
III. To create an enabling environment that attracts hyperscaler and data centre investments through regulations and incentives.
IV. To ensure the security, transparency, and sovereignty of Nigeria's cloud ecosystem in alignment with national and international standards.
V. To provide a framework for compliance with Presidential Executive Orders 003 (2017) and 005 (2018) on local content and the promotion of Nigerian enterprise.
VI. To establish a baseline of current cloud adoption across FPIs and implement a robust framework to measure and report on progress towards achieving a 75% adoption rate by 2030.

8 In this Guideline, unless the context otherwise requires, the following terms shall have the meanings assigned to them below: **Definitions**

Bureau of Public Procurement (BPP) means the primary public procurement regulator under the Public

Procurement Act, 2007.

Capital Expenditure (CapEx) means upfront investment in fixed IT assets or infrastructure, as opposed to operational subscription models.

Cloud First means a directive requiring FPIs to prioritise cloud-based solutions over on-premises alternatives when procuring or deploying new IT resources, unless there is a clear, documented justification.

Cloud Readiness Assessment means a structured evaluation of an FPI's ability to migrate to the cloud, covering security, lifecycle, legal, technical, and operational factors.

Cloud Service Provider (CSP) means an entity that offers cloud computing services (IaaS, PaaS, SaaS) and is contractually responsible for service levels and security of those services. CSP may operate its own infrastructure or use contracted facilities/partners. This includes large-scale providers often referred to as hyperscalers.

Data Breach means any confirmed or suspected incident leading to unauthorized access, disclosure, alteration, or destruction of data processed under this Guideline.

Data Controller / Processor shall have the meanings assigned to them under the NDPA 2023, whereby a controller determines the purpose and means of processing, while a processor acts on behalf of the controller. CSPs and SIs may be either, depending on contractual roles.

Data Residency means the physical or geographical location of an organisation's data or information.

Data Sharing Agreement (DSA) means a legally binding agreement between FPIs governing the lawful basis, scope, security, and auditability of inter-agency

data exchanges, as required under Ne-GIF.

Federal Public Institution (FPI) means any Ministry, Department, or Agency of the Federal Government of Nigeria, including any unit that processes government data under mandate or contract.

Financial Operations (FinOps) means principles applied to cloud cost optimisation, including continuous monitoring, right-sizing, and savings instruments.

Government-designated Aggregation Entity means the entity designated by the Federal Government to perform the functions of cloud aggregation, demand consolidation, negotiated procurement, and related functions under this Guideline. Until otherwise designated by the Federal Government, Galaxy Backbone Limited (GBB) shall serve as the Government-designated Aggregation Entity.

Hybrid Cloud means a deployment model that combines private and public cloud infrastructure, where sensitive data may be kept in private environments and other workloads in public or community clouds.

Infrastructure-as-a-Service (IaaS) means a cloud service model that provides virtualised computing resources, such as servers, storage, and networking.

Indigenous Provider / Indigenous Cloud Service Providers / Indigenous Service Integrator means a CSP or SI incorporated in Nigeria and certified by NITDA as compliant with local content requirements as prescribed in the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2019. Foreign CSPs may be granted provisional indigenous status under strategic investment rules. Any other CSP or SI that does not meet these criteria is considered a Foreign CSP or SI.

Latency / Access Benchmarks means nationally or internationally recognised standards for network speed and reliability required to ensure government and regulated sector data services hosted in the cloud remain accessible to end-users.

Mutual Legal Assistance Treaty (MLAT) means an international agreement that establishes lawful frameworks for cross-border government-to-government data access requests.

Nigeria Data Protection Act (NDPA), 2023 means the national law governing personal data processing and cross-border transfers in Nigeria.

Nigeria Data Protection Commission (NDPC) means the statutory body mandated to enforce NDPA compliance.

Nigerian e-Government Interoperability Framework (Ne-GIF) means the federal framework for ensuring cross-agency systems can securely exchange data.

National Information Technology Development Agency (NITDA) means the Agency established under the National Information Technology Development Agency Act, 2007, and the lead coordinating body for the implementation of this Guideline.

Office of the National Security Adviser (ONSA) means the lead authority on matters of national security, particularly Level 4 classified data.

Operational Expenditure (OpEx) means ongoing subscription-based or pay-as-you-go IT costs as opposed to upfront CapEx investments.

Platform-as-a-Service (PaaS) means a cloud service model that provides platforms and runtime environments for developing, testing, and deploying applications.

Privacy Impact Assessment / Data Protection Impact Assessment (PIA / DPIA) means the required assessments under the NDPA for new systems processing personal data.

Public-Private Partnership (PPP) means a contractual collaboration between the government and private entities for infrastructure or service delivery.

Role-Based Access Control (RBAC) means a security principle that requires that users be granted only the access rights strictly necessary to perform their duties.

Recovery Point Objective (RPO) means the maximum acceptable amount of data loss measured in time (e.g., last 4 hours of data).

Recovery Time Objective (RTO) means the maximum acceptable downtime after a disruption before services must be restored.

Regulated Sector means any sector of the economy that is subject to the oversight, supervision, licensing, registration, or regulation of a competent statutory or regulatory authority established under any applicable law in Nigeria, including sectors designated as critical to national security, public safety, financial stability, public health, or the delivery of essential public services.

Software-as-a-Service (SaaS) means a cloud service model in which software applications are delivered over the internet on a subscription basis.

Sovereign Infrastructure means digital infrastructure that satisfies prescribed requirements for jurisdictional control, data residency, operational control, security, auditability, resilience, and compliance with applicable Nigerian laws and regulatory instruments.

Sovereign Compute means compute infrastructure

designed to support sensitive, critical, artificial intelligence, high-performance computing, or strategically important workloads in a manner that preserves Nigerian jurisdictional control, security, and operational resilience.

Digital Regulatory Platform (DRP) means the digital platform established by the Agency for the administration of regulatory, registration, certification, licensing, assurance, compliance, monitoring, and other digital regulatory services, including such modules and services as the Agency may prescribe from time to time.

Schedule A means the National Data Classification Framework (part of this Guideline).

Schedule B means the Cloud Service Provisioning and Procurement Guidelines (part of this Guideline).

Schedule C means the Cloud Migration and Deployment Framework (part of this Guideline).

Schedule D means the National Cloud Governance Framework (part of this Guideline).

Service Integrator (SI) means a legal entity, including a company, partnership, or registered business name with the Nigerian Corporate Affairs Commission, or a consortium led by such an entity, that plans, designs, procures, implements, configures, supports, and manages cloud solutions for customers, often by integrating services from one or more CSPs. SIs are delivery and integration partners engaged within the aggregated framework agreements established under the National Cloud Computing Guideline and are provisioning entities for government and regulated sector services under this Guideline.

Service Level Agreement (SLA) means a contractual agreement specifying minimum service levels, security requirements, penalties, liability, and exit strategy

provisions between an FPI and its CSP/SI.

Shared Responsibility Model means the framework, as defined in Schedule D, that delineates responsibilities of CSPs, FPIs, and SIs.

Sovereign Cloud Governance Committee (SovGov) means the inter-agency and stakeholder advisory and coordination mechanism established to support the implementation of the National Cloud Computing Guideline and promote coordinated oversight of government and regulated sector cloud adoption

Strategic Investment Waiver means a temporary localisation waiver granted by NITDA on the recommendation of SovGov to a foreign CSP that commits to significant, verifiable, time-bound investments in local data centre and cloud infrastructure.

Vendor Lock-in means a condition where an FPI becomes dependent on a single provider, unable to easily migrate to another CSP due to technical, contractual, or financial barriers.

9 9.1 Cloud First Principle

Core Guideline Directives

The Federal Government mandates a **"Cloud First"** approach for all Federal Public Institutions (FPIs). This means FPIs shall prioritise cloud-based solutions as the primary option when procuring and deploying new IT resources. This directive aims to reduce capital costs, improve service delivery, and increase efficiency across the public sector.

Where an FPI seeks to retain or deploy an on-premises or non-cloud environment contrary to the Cloud First Principle, the institution shall document the technical, operational, security, regulatory, financial, or sovereignty justification and obtain NITDA approval in accordance with prescribed procedures.

In implementing this directive, priority consideration

must be given to Indigenous Cloud Service Providers (CSPs). A foreign CSP may be granted provisional indigenous status for procurement purposes by NITDA if they have made suitable strategic investments within the country. The determination of a "suitable investment" is made by the **Sovereign Cloud Governance Committee (SovGov)**, as established in **Schedule D**, using the evaluation framework found in **Annex H of the National Cloud Technical Guideline**.

All related procurement activities must be conducted in accordance with the complete process detailed in **Schedule B: Cloud Service Provisioning and Procurement Guidelines for FPIs**. All such procurements must also comply with the Public Procurement Act, 2007 (as amended) and the Bureau of Public Procurement (BPP) regulations and guidelines. In case of conflict, the PPA/BPP shall prevail.

Procurement by FPIs under this Guideline shall be executed through the aggregated framework agreements established under the National Sovereign Cloud Policy, with registered Service Integrators engaged as delivery and integration partners within such agreements. Direct procurement outside the aggregation framework shall require the exception clearance prescribed under that Policy.

9.2 Data Classification and Transfers

This framework applies to government-held data, regulated sector data, public interest data, and other non-personal data categories which the NDPA does not specifically address, and categorises them based on sensitivity. Accordingly, a national data classification framework is hereby established, as detailed in **Schedule A: National Data Classification Framework**.

Data transfers across borders are permissible only when fully compliant with the NDPA and this Guideline's stipulations. The framework defines thresholds for localisation and exceptions for cross-border flows to

balance security with the need for global collaboration.

Access to sovereign data by foreign entities, including foreign governments, shall be strictly governed by the provisions of the NDPA and formal Mutual Legal Assistance Treaties (MLATs) or similar diplomatic instruments. Direct requests for data access shall not be granted outside of these legal channels.

This Guideline does not restrict cross-border transfers of metadata or operational data required by certified CSPs for service support, uptime, security, and analytics, provided such transfers comply with the NDPA on personal data. The specific guidelines governing these operational transfers are detailed in the **National Cloud Technical Guideline**.

Notwithstanding any other provision of this Guideline, all financial data generated, processed, transmitted or stored by regulated financial institutions shall be primarily hosted, processed and stored within the territorial boundaries of the Federal Republic of Nigeria.

9.3 Data Sovereignty and Residency

Nigeria asserts its sovereign right to govern data processed and stored within its territory. All sovereign data classified as Level 2 and above, as defined and categorised in **Schedule A: National Data Classification Framework**, shall be hosted within Nigeria by default, subject to temporary waivers as provided below.

Data controllers and processors must comply with the specific Data Residency and hosting requirements stipulated for each data classification level within Schedule A. Temporary waivers for data localisation may only be granted to CSPs by NITDA as part of a strategic investment initiative, as detailed in Schedule D.

Infrastructure supporting sensitive, strategic, or critical government and regulated sector workloads shall satisfy applicable sovereign infrastructure requirements,

including jurisdictional control, data residency, operational and administrative control, technical and security compliance, auditability, transparency, resilience, and continuity arrangements.

For the avoidance of doubt, infrastructure shall not be deemed sovereign solely on the basis of physical location, ownership structure, or commercial description. Qualification shall be based on requirements prescribed by NITDA under applicable standards, certification, and assurance frameworks.

Nothing in this Guideline shall derogate from sector-specific legal or regulatory requirements relating to data classification, data localisation, cybersecurity, operational resilience, supervisory access, records retention, or other statutory obligations issued by competent sector regulators.

Sector regulators may adopt additional safeguards or classify data at a higher level than the baseline classification prescribed under this Guideline but shall not assign a lower classification or reduce the minimum protection requirements established herein.

Where sector-specific requirements impose higher or additional obligations, regulated entities shall comply with such requirements.

9.4 Future-Proofing and Scalability

This Guideline promotes the adoption of cloud architectures and standards that are inherently scalable and adaptable to future technological advancements.

I. **Scalability**: All cloud services procured by Federal Public Institutions (FPIs) must be able to scale on-demand. This ensures that digital public services can efficiently handle fluctuations in user load, manage costs effectively by paying only for resources consumed, and maintain optimal performance as demand grows.

II. **Future-Proofing**: To avoid technological obsolescence and prevent vendor lock-in, the Guideline mandates a commitment to **open**

standards and interoperability.

NITDA shall conduct periodic reviews and updates of the technical standards to incorporate emerging technologies and ensure the long-term viability of Nigeria's sovereign cloud ecosystem.

NITDA shall retain responsibility for updating and maintaining the technical standards that accompany this Guideline.

9.5 International Cooperation and Alignment

This Guideline is designed to be interoperable with global standards and international government frameworks to facilitate digital trade and cross-border collaboration.

However, any adoption of or alignment with international trade agreements, data transfer frameworks, or foreign government regulations is contingent upon a thorough assessment by NITDA. Such agreements shall only be approved if they demonstrably support Nigeria's sovereign interests, economic development objectives, and the security of the national digital ecosystem.

The primary goal is to ensure that international cooperation enhances, rather than compromises, Nigeria's national goals.

10 Security, Privacy, and Risk Management

10.1 Data Privacy and Protection

All personal data processing shall comply with the Nigeria Data Protection Act (NDPA) 2023 and its implementation directives. This includes respecting the principles of fairness, lawfulness, and transparency, and safeguarding the rights of data subjects. Cloud Service Providers (CSPs) are legally obligated to protect the confidentiality, integrity, and availability of data hosted on their platforms.

10.2 Risk Management Framework

Entities shall undertake risk-based due diligence to identify and mitigate potential adverse impacts arising from cloud services, including risks from technical

dependencies on foreign-developed software. A comprehensive risk assessment shall be completed before migrating services to the cloud, as specified in the **National Cloud Technical Guideline**.

10.3 Incident Response and Recovery Planning

To ensure the continuity of public services and the resilience of national digital infrastructure, all CSPs and Service Integrators (SIs) shall develop, implement, and periodically test standardised incident response and disaster recovery plans. These plans must define clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) and include procedures for regular disaster recovery simulations to validate readiness against security breaches, service outages, and other disruptions. The specific technical requirements for these plans, including minimum RTO/RPO targets and testing frequencies, are detailed in the **National Cloud Technical Guideline.**

10.4 Liability and Resolution of Issues

In line with the Shared Responsibility Model defined in Schedule D, CSPs and SIs shall be held contractually and statutorily liable for breaches of contract and for data breaches that result from non-fulfilment of their assigned security, operational, and infrastructure obligations.

10.5 Intra-Governmental Data Access

Access by one FPI to data held by another FPI shall be prohibited unless expressly authorised under law. However, to facilitate government operations, two distinct pathways for data sharing are established:

I. **Routine Operational Sharing:** To enhance operational efficiency for routine and pre-defined exchanges, the implementing authority of the Nigerian e-Government Interoperability Framework (Ne-GIF) may facilitate and approve access between FPIs, subject to a legally-vetted Data Sharing Agreement (DSA) between the participating agencies. The Ne-GIF authority shall certify that proper compliance, immutable audit trails, and verifiable security controls are in place

before granting access.

II. **Sensitive and Ad-Hoc Sharing:** For any ad-hoc or sensitive data access requests that fall outside the scope of an established DSA, access shall require an order of a court of competent jurisdiction or other lawful authorisation recognised under applicable Nigerian law.

III. Inter-agency data sharing shall, where applicable, leverage the Nigeria Data Exchange (NGDX) or any other approved national data exchange mechanism to support secure, consent-based, auditable, and interoperable data exchange between Federal Public Institutions.

10.6 Continuous Compliance Audits

To ensure ongoing adherence to national standards, all CSPs and SIs engaged with FPIs shall be subject to periodic compliance audits conducted by a NITDA-certified auditor.

These audits are intended to confirm compliance with the NDPA, Service Level Agreement (SLA) commitments, and the security standards established by this Guideline. The specific mechanisms, scope, and procedures for these audits are detailed in **Schedule D: National Cloud Governance Framework.**

11 Service and Operational Principles

11.1 Access and Connectivity Standards

Cloud services shall be designed and deployed to be universally accessible, ensuring equitable service availability for all citizens. Entities shall ensure that cloud deployments do not, whether directly or indirectly, create barriers for individuals in underserved or disadvantaged regions.

11.2 Cloud and Data Portability

To prevent vendor lock-in, FPIs shall ensure that contracts and technical architectures guarantee the migration of data and applications between different CSPs. Compatibility with open standards should be

prioritised in procurement.

All cloud contracts shall include documented exit and transition arrangements, including data extraction formats, migration assistance obligations, transition timelines, deletion or return of data, and measures to minimise vendor lock-in.

11.3 Interoperability Requirements

Cloud infrastructure components shall support interoperability to allow systems from different providers to work together, based on the Nigerian e-Government Interoperability Framework (Ne-GIF) and international standards.

To prevent vendor lock-in at the application layer, all PaaS and SaaS solutions procured by FPIs shall comply with **open APIs and data exchange standards (e.g., REST, JSON, XML),** as prescribed in the National Cloud Technical Guideline, to ensure seamless integration and data portability between government systems.

11.4 Mandate for Service Level Agreements (SLAs)

All cloud services procured by Entities shall be procured and governed by legally binding SLAs that expressly define performance expectations, penalties for non-fulfilment, and provisions for data protection, in accordance with the minimum requirements set forth in **Schedule B: Cloud Service Provisioning and Procurement Guidelines.**

12 Governance and Implementation

12.1 National Cloud Governance Framework

A **Sovereign Cloud Governance Committee (SovGov)** is hereby established as an advisory body to support the implementation and enforcement of this Guideline. NITDA shall serve as the lead implementing and coordinating authority for the governance of this Guideline, coordinating with the Bureau of Public Procurement (BPP), the Office of the National Security Adviser (ONSA), and other relevant bodies. The roles, responsibilities, and decision-making hierarchy shall be

as defined in **Schedule D: National Cloud Governance Framework.** This framework ensures that cloud usage and expenditures align with agency objectives and national priorities.

12.2 Implementation Guidelines & Compliance Support

To ensure the successful and consistent application of this Guideline, NITDA will develop, maintain, and periodically update a suite of implementation guidelines and support materials.

These implementation guidelines shall translate this Guideline and its Schedules into detailed, actionable compliance frameworks to aid in nationwide compliance. This shall include, but is not limited to:

a. A detailed Data Classification and Residency Implementation Guideline.
b. Technical best practices for cloud migration and deployment.
c. Security and risk management protocols.
d. Templates for procurement and Service Level Agreements (SLAs).
e. A Cloud Appropriateness Checklist to assist FPIs in documenting the operational, financial, security, and risk-based considerations underpinning their cloud and deployment model decisions, particularly in identifying the limited circumstances in which an alternative deployment model is more suitable for a specific workload.
f. A defined grace period for FPIs to build capacity, inventory their data assets and develop phased migration plans for non-compliant services.
g. Cloud adoption and migration activities shall take into account the availability, maturity, and readiness of compliant cloud and digital infrastructure capable of supporting the relevant workload, service level, security, and data classification requirements.

The development of these materials shall be informed by comprehensive needs analyses and broad stakeholder consultations to ensure they remain relevant and effective. The initial Data Classification and Residency Implementation Guideline must be published within twelve (12) months of this Guideline's effective date, with other support materials issued thereafter on a rolling basis. These and other resources shall be made readily available via the NITDA Digital Regulatory Platform.

Implementation of this Guideline shall adopt a phased approach, taking into consideration infrastructure availability, workload criticality, institutional readiness, risk consideration, and national priorities.

NITDA may establish assessment, certification, assurance, and onboarding frameworks to support the implementation of this Guideline, including requirements for cloud service providers, service integrators, data centre operators, and other digital infrastructure providers serving Federal Public Institutions.

12.3 Financial Operations (FinOps) and Cost Management

FPIs shall transition from capital expenditure (CapEx) based IT procurement in favour of an operational expenditure (OpEx) model, with cloud contracts structured on a consumption-based ("pay as you go") basis to optimise spending.

To support whole-of-government cloud aggregation and realise economies of scale, the Government-designated aggregation entity shall have the authority to aggregate cloud usage and consumption data across Federal Public Institutions (FPIs) through the Digital Regulatory Platform to:

a. Negotiate whole-of-government cloud procurement and purchase agreements;

b. Drive cost efficiencies and optimise the utilisation of

cloud resources across government;

c. Implement negotiated pricing, chargeback, and other cloud aggregation mechanisms established under the National Sovereign Cloud Policy; and

d. Promote and disseminate best practices, standards, and guidance on cloud adoption and management across all tiers of government, including the Federal, State, and Local Governments.

12.4 Environmental Sustainability

This Guideline promotes the adoption of green cloud technologies. Entities shall give preference to certified providers that utilise energy-efficient data centres and renewable energy solutions to reduce the national carbon footprint.

12.5 Awareness and Sensitisation

NITDA shall promote awareness, sensitisation, and capacity-building programmes to support the effective implementation of this Guideline by Federal Public Institutions, cloud service providers, service integrators, and other relevant stakeholders.

13 Compliance and Enforcement

13.1 Data Sovereignty Compliance Framework

A compliance model is hereby established to enforce data residency, classification, and security obligations. This shall include monitoring tools, standardised audit protocols, and a certification pathway for CSPs as specified in the **National Cloud Technical Guideline and the National Digital Infrastructure Assurance Framework (NDIAF).**

13.2 Penalties and Sanctions

Any breach of the provisions of this Guideline is a violation of the NITDA Act, 2007 and enforceable under its provisions.

NITDA shall impose sanctions based on the principle of proportionality, taking into account the severity, impact, and nature of the violation. The enforcement framework shall comprise the following graduated measures:

a. **Administrative Actions:** For minor administrative or procedural issues, NITDA may issue a formal warning and require the submission of a corrective action plan.
b. **Contractual and Certification Actions:** For more significant operational or compliance failures, NITDA may apply administrative measures, temporarily suspend a provider's services from the Digital Regulatory Platform, and/or mandate a formal recertification audit.
c. **Without Prejudice to Statutory Penalties:** The administrative and contractual sanctions under this Guideline are distinct from and do not supersede the penalties for data breaches or cybercrimes as stipulated in other laws such as the Nigeria Data Protection Act (NDPA) 2023 and the Cybercrimes (Amendment) Act 2024. Non-compliance with these laws shall attract penalties and remedies as prescribed therein.

Without prejudice to the powers of other competent authorities, NITDA may issue advisories, remediation notices, compliance directives, suspension notices, and other administrative measures in accordance with the NITDA Act.

Nothing in this Guideline shall prejudice the statutory powers of other competent regulators. NITDA shall coordinate with relevant authorities to ensure effective compliance and enforcement.

This Guideline shall be reviewed every three (3) years or earlier as may be determined by NITDA to reflect technological developments, implementation experience, emerging risks, and changes in applicable laws or national priorities.

SCHEDULES TO NATIONAL CLOUD COMPUTING GUIDELINE

14	**14.1. Schedule A: National Data Classification Framework**	**Purpose**

This Framework is founded on the principle that data is a strategic national asset requiring appropriate governance throughout its lifecycle. Accordingly, all organisations and entities within the scope of this Framework shall establish and maintain the capability to effectively govern the data under their custody or control. This shall begin with the identification and maintenance of an inventory of data assets to understand their nature, value, ownership, sensitivity, and criticality.

Building on this foundation, the Framework establishes a mandatory data classification system to ensure that government, regulated sector, and citizen data are managed, stored, processed, and protected in accordance with their sensitivity, criticality, and associated risks. It provides a consistent methodology for data classification and risk management, supports compliance with applicable laws and regulatory requirements, including the Nigeria Data Protection Act, 2023, where personal data is concerned, and serves as the foundation for implementing Nigeria's data sovereignty, residency, security, and cloud governance requirements.

14.2. Data Classification Levels

All government, citizen, corporate, and regulated sector data must be classified into the following levels, organised by sensitivity. This classification also applies to public interest and other non-personal data categories.

Level	Sensitivity	Data Type Examples	Hosting/Residency Requirement	Localisation Requirement Nature
Level 4	Classified	Military intelligence, Critical National Information Infrastructure (CNII), strategic national secrets	Data shall be hosted exclusively on-premise within the FPI, in a collocated private data centre, or in a government-certified private cloud located within Nigeria	Stringent/ Mandatory
Level 3	Highly Sensitive	Regulated sectors data and sensitive personal information including data with potential impact on national interest, including but not limited to data from Public-Private Partnerships (PPPs) and designated CNII. Inter-governmental communications, internal memos and related records fall under Level 3.	Data shall be primarily hosted in a private or secure hybrid cloud within Nigeria's territorial boundary. Cross-border transfer for sensitive personal data is permissible only under lawful transfer mechanisms recognised under the NDPA	Mandatory
Level 2	Sensitive	Personal health and social information	Data shall be hosted in a cloud environment within Nigeria's territorial boundary by default. Cross-border hosting shall only be permitted with prior authorisation from	Highly Recommended

			NITDA, and shall be subject to any lawful transfer mechanism recognised under the NDPA. The receiving jurisdiction must also maintain adequate data protection standards and meet nationally or internationally recognised latency and access requirements.	
Level 1	Open	Open government data, public reports, personally shared information	Data may be hosted in a public cloud environment that complies with national or internationally recognised information security standards	Flexible

15 15.1. LEVEL 4 - CLASSIFIED

Classification Levels

I. **National Security Data**

a. **Sensitivity Level:** Classified

b. **Description:** Data vital to national security or strategic national interests, the compromise of which poses a direct and significant threat to national safety, stability, defence, or the economy.

c. **Examples:** Military intelligence, law enforcement investigation data, critical national infrastructure schematics, strategic national secrets, and diplomatic communications of a sensitive nature.

d. **Hosting Requirement:** Data shall reside

exclusively on-premises within the FPI, in a collocated private data centre, or in a NITDA-certified private cloud located within Nigeria's territorial boundary. The hosting infrastructure must comply with security standards defined and audited by the Office of the National Security Adviser (ONSA) and requirements in the **National Cloud Technical Guideline**.

e. **Data Retention & Erasure:** Retention periods shall be determined by applicable national security directives and laws. Erasure shall follow a certified, secure, and auditable destruction protocol to ensure irrecoverability.

15.2. LEVEL 3 - HIGHLY SENSITIVE

I. **Public Sensitive Data**

a. **Sensitivity Level:** High

b. **Description:** Regulated sector data which, if compromised, could significantly affect national security, or the economy.

c. **Examples:** Critical economic data, payment transaction records, strategic policy documents, and regulated industry information which, if prematurely disclosed, may constitute market manipulation, confer unfair competitive advantage, or disrupt orderly governance.

d. **Hosting Requirement:** Data shall be primarily hosted in a private or secure hybrid cloud within Nigeria's territorial boundary, protected by strong encryption and access controls. Cross-border transfer/hosting of sensitive personal information is permissible only under NDPA-compliant conditions and subject to NITDA approval, where applicable.

e. **Data Retention & Erasure:** Data shall not be retained beyond what is strictly necessary for its lawful purpose. Retention policies shall be documented, clearly defined and auditable. Erasure shall be effected using secure and verifiable data sanitisation methods.

II. **Corporate Confidential Data**

a. **Sensitivity Level:** High
b. **Description:** Confidential corporate or commercial data which, if disclosed, could materially harm economic interests or national security. NITDA and ONSA may designate specific private sector data as Level 3 when critical to national interest, subject to due process and applicable oversight.
c. **Examples:** Proprietary industry data, sensitive financial market information, data from PPPs, data from CNII, and trade secrets vital to the national economy.
d. **Hosting Requirement:** Data shall be hosted in a private or secure hybrid cloud within Nigeria's territorial boundary, with security measures equivalent to those required for Public Sensitive Data.
e. **Data Retention & Erasure:** Data shall not be retained beyond the period strictly necessary for its lawful purpose. Retention policies shall be documented, clearly defined, and auditable. Erasure shall be effected using secure and verifiable data sanitisation methods.

15.3. LEVEL 2 - SENSITIVE

I. **Private Sensitive Data or Confidential**

a. **Sensitivity Level:** Moderate
b. **Description:** Personal data of individuals, or confidential data of public institutions and SMEs, that is not high-risk but requires protection against harm or breach of privacy.
c. **Examples:** Sensitive personal data as defined by the NDPA, confidential reports, and internal records of public institutions or SMEs.
d. **Hosting Requirement:** Data may reside in a cloud environment within Nigeria’s territorial boundary or, subject to the NDPA, abroad based on explicit consent or other lawful basis,

provided the host jurisdiction maintains adequate protection standards and recognised low-latency and access benchmarks.

e. **Data Retention & Erasure:** Retention shall be limited to the minimum necessary for the purpose for which it was collected. Data must be securely deleted upon a valid erasure request or once the purpose is fulfilled.

II. **Private Insensitive Data**

a. **Sensitivity Level:** Moderate
b. **Description:** Personal data not classified as sensitive but still subject to NDPA protections, including non-sensitive data held by public institutions and SMEs.
c. **Examples:** Basic personal identification information, non-sensitive records held by public institutions, and general operational data of SMEs.
d. **Hosting Requirement:** Data may reside in a cloud environment within Nigeria's territorial boundary, or abroad subject to NDPA compliance and recognised standards for low latency and accessibility.
e. **Data Retention & Erasure:** Retention policies must comply with the NDPA. Standard secure deletion practices are required upon the expiration of the retention period.

15.4. LEVEL 1 - OPEN

I. **Public Insensitive Data**

a. **Sensitivity Level:** Low
b. **Description:** Publicly available information or data approved for public release, the disclosure of which poses no risk of harm.
c. **Examples:** Official publications, open government data, public directories, and information intended for the general public.
d. **Hosting Requirement:** Data may be hosted in a public cloud environment that complies with national or globally recognised information

security standards.

e. **Data Retention & Erasure:** May be retained indefinitely for public archival purposes in accordance with national archival laws. Standard deletion practices are sufficient if erasure is required.

II. **Corporate Non-Confidential Data**

a. **Sensitivity Level:** Low

b. **Description:** General non-confidential business information from industry, private, or public sector entities that is not confidential and is intended for public dissemination.

c. **Examples:** Corporate annual reports, marketing materials, public-facing product information.

d. **Hosting Requirement:** Data may be hosted in a public cloud environment that complies with national or internationally recognised information standards.

e. **Data Retention & Erasure:** Retention is determined by the business relevance of the data. Standard deletion practices shall apply where erasure is required.

16 Responsibilities of FPIs, CSPs and SIs

Responsibilities

This section outlines the primary responsibilities of the key actors within Nigeria's sovereign cloud ecosystem. Additional role-specific duties are detailed in other sections of this Guideline and its schedules.

16.1. Responsibilities of Federal Public Institutions (FPIs)

Each FPI is responsible for the governance and management of its own data assets. In addition to the responsibilities for guideline implementation outlined in **Schedule D**, FPIs must:

I. **Data Classification:** Inventory and classify all data assets in accordance with the mandatory classification framework in **Schedule A: National Data**

Classification Framework. To ensure correctness, the data classification results must be shared with NITDA.

II. **Data Retention:** FPIs shall establish retention schedules with maximum permissible timeframes for each classification level, except where overridden by statutory or national security requirements.

III. **Oversight and Compliance:** The designated Data Protection Officer (DPO) within each FPI shall oversee the data classification process, ensure its implementation, and report on compliance as part of their duties under the NDPA.

IV. **Procurement and Contracts:** Ensure all procurement of cloud services adheres strictly to the guidelines in **Schedule B: Cloud Service Provisioning and Procurement Guidelines for FPIs**, including all contractual and SLA requirements.

V. **Data Sharing for Guideline Oversight:** FPIs are mandated to share necessary operational, consumption, and compliance data with NITDA upon request. This data sharing is required to enable effective monitoring and tracking of this Guideline's implementation and to allow NITDA to identify opportunities for shared services and other beneficial cross-government solutions.

16.2. Responsibilities of Cloud Service Providers (CSPs)

All CSPs handling government and regulated sector data are contractually obligated to adhere to this Guideline. They must:

I. **Implement Security Controls:** Implement and enforce the technical and security controls appropriate for the specific data classification level of the information they process or store, as detailed in the **National Cloud Technical Guideline**.

II. **Enable FPI Compliance:** Provide FPIs with the necessary service configurations and management tools to allow them to manage their data according to its classification.

III. **Meet Hosting Requirements:** Ensure their infrastructure and services comply with data residency and hosting requirements for each classification level in **Schedule A**. CSP contracts must include minimum service-level provisions covering breach notification, liability, and audit rights.

16.3. Responsibilities of Service Integrators (SIs)

All SIs that deploy, configure, or manage cloud services on behalf of an FPI are contractually obligated to adhere to this Guideline. They must:

I. **Adhere to Classification:** Implement and manage cloud environments in strict accordance with the FPI's data classification decisions.
II. **Uphold Shared Responsibility:** Fulfil their duties within the **Shared Responsibility Model**, as defined in the SLA, ensuring the secure configuration of cloud services, management of access controls, and protection of applications they deploy.
III. **Maintain Technical Standards:** Ensure all configurations and deployments comply with the minimum standards outlined in the **National Cloud Technical Guideline**.

17 Schedule B: Cloud Service Provisioning and Procurement Guidelines for FPIs

Purpose

These guidelines establish a standardised and mandatory process for the procurement of cloud services by FPIs. The process is designed to ensure transparency, value for money, compliance with the "Cloud First" Principle, and prioritisation of local content.

17.1. The Digital Regulatory Platform

The Digital Regulatory Platform managed by NITDA is the mandatory and exclusive portal for the procurement of all cloud services by Federal Public Institutions (FPIs).

I. **Purpose:** The Digital Regulatory Platform is designed to:
   a. **Ensure Transparency:** Provide a single, open platform for FPIs to discover, compare, and procure certified cloud services.
   b. **Promote Competition:** Foster a competitive environment among certified providers, ensuring value for money.
   c. **Simplify Procurement:** Streamline the procurement lifecycle from service discovery to contract management in alignment with the Public Procurement Act, 2007.

II. **Listing of Services:** Only Cloud Service Providers (CSPs) and services that have been certified by NITDA as compliant with the National Cloud Computing Guideline and its technical standards shall be listed on the Digital Regulatory Platform. FPIs are prohibited from procuring cloud services from unlisted providers and any such contracts shall be subject to administrative sanctions by NITDA and BPP.

III. **Publication of Digital Regulatory Platform Listing Process:** NITDA shall develop, approve, and publish the detailed process, criteria, and technical requirements for the certification and listing of CSPs and their services on the Digital Regulatory Platform.

IV. This complete directive shall be made publicly available on the official NITDA website and the Digital Regulatory Platform no later than **three (3) months** from the effective date of this Guideline.

17.2. Procurement Process

I. **Needs Assessment and Justification:** FPIs must first conduct a thorough assessment of their IT requirements and justify the need for a cloud-based solution, considering potential gains in efficiency, agility, and innovation. Where the assessment concludes that cloud deployment is operationally infeasible or economically unjustifiable for the specific workload, the FPI shall document the rationale, propose an alternative deployment model, and submit the justification to NITDA for review and concurrence as part of the IT Project Clearance Process.

II. **NDPA Compliance:** Each FPI shall conduct a Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA) in accordance with the NDPA prior to procurement.

III. **Review and Sourcing:** Procurement of cloud services must be conducted through the Digital Regulatory Platform for cloud service providers. This portal, managed by NITDA, will contain a list of pre-approved CSPs and their service offerings, enabling transparent comparison.

IV. **Data Classification Alignment:** The chosen cloud service and deployment model (public, private, hybrid) must align with the classification level of the data to be hosted, as stipulated in **Schedule A: National Data Classification Framework**.

V. **Local Content Priority:** In line with the Guidelines for Nigerian Content Development in ICT, preference for new cloud procurement must be granted to indigenous CSPs. To qualify for such priority, indigenous CSPs must be certified by NITDA and listed on the Digital

Regulatory Platform as detailed in **Schedule C: Cloud Migration and Deployment Framework for FPIs**. Indigenous CSPs are encouraged to provide standard FPI-focused service bundles on their websites that can be linked to the Digital Regulatory Platform, for ease of procurement.

a. Foreign CSPs may only be engaged if: (a) NITDA verifies in writing that no local capacity exists for the required service; or (b) a foreign CSP obtains **provisional indigenous status** by making a suitable investment in local data centre infrastructure. Criteria for what constitutes a "suitable investment" shall be objective, measurable, and published by NITDA, rather than discretionary, to prevent abuse, ensure predictability, and align with national development objectives. Where provisional indigenous status involves hosting outside Nigeria during the initial investment period, the provider must obtain a **Data Localisation Waiver under Schedule D, section 19.2(III)(d).** For guidance, a framework for evaluating strategic investments is provided in **Annex H of the National Cloud Technical Guideline**.

b. A government-invested or partially government-owned CSP is considered an indigenous provider and will be granted the same priority consideration. All priority considerations under this provision are contingent upon the provider meeting the requisite technical, security, and pricing benchmarks as detailed in the **National Cloud Technical Guideline** and verified during their certification for the Digital Regulatory Platform.

VI. **Contracting and Financial Model:** All cloud service contracts shall be structured on a consumption ("pay as you go") or subscription basis to align with an operational expenditure (OpEx) model. Contracts must

include clear provisions to prevent vendor lock-in and shall incorporate a comprehensive Service Level Agreement (SLA) that meets the minimum requirements laid out in section 17.3 below.

VII. **Bid Evaluation:** Procurement bids from SIs must be evaluated with a clear separation between the cost of cloud infrastructure consumption and the cost of the SI's management, integration, support and other non-core services. This unbundling ensures fair and transparent comparison of service costs, especially where underlying cloud infrastructure is procured via whole-of-government agreements.

17.3. Minimum SLA Requirements

SLAs are mandatory for all cloud service contracts and must clearly define, at a minimum:

I. **Availability and Performance:** Minimum uptime guarantees (e.g., 99.9%), latency benchmarks, and response times (especially for data hosted outside the country's territorial boundaries, e.g., Level 2 and Level 1).

II. **Data Protection and Security:** Explicit commitment to adhere to the NDPA 2023, specifying data location, encryption standards, and procedures for data breach notification.

III. **Business Continuity and Disaster Recovery:** Detailed disaster recovery protocols, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

IV. **Technical Support Requirements:** Clearly defined tiers of support, guaranteed response and resolution times based on issue severity, hours of operation (e.g., 24x7x365 for critical issues), and clear escalation procedures, including escalation to NITDA where breaches remain unresolved beyond defined operational thresholds.

V. **Penalties for Non-Performance:** A clear penalty clause for any failure to meet agreed-upon service levels. While this Guideline does not mandate uniform penalty values, it requires that remedies, typically in the form of **service credits**, be clearly defined. This approach allows providers to use their standard global SLA terms while ensuring FPIs have a clear recourse for non-performance. In addition to service credits, SLAs must specify circumstances constituting material breach entitling the FPI to terminate the contract and seek damages. A sample SLA template is available for reference in Annex B of the **National Cloud Technical Guideline**.

VI. **Data Ownership and Exit Strategy:** A clause affirming that the entity retains full ownership of its data at all times. An exit strategy schedule must specify maximum timelines (not exceeding 90 days) for the secure and complete repatriation, transfer, and/or deletion of all government and regulated sector data upon contract expiration or termination. The Exit Strategy Schedule shall be appended to the contract as a mandatory exhibit, specifying supported export formats, the SI's migration responsibilities, and anti-lock-in audit provisions.

VII. **Shared Responsibility Model:** The SLA must explicitly define the security responsibilities of both the CSP and the FPI. It must clarify that the CSP is responsible for the "security *of* the cloud" (i.e., the infrastructure), while the FPI is responsible for the "security *in* the cloud" (i.e., data, access controls, configurations, and applications).

/III. **Review of Existing Agreements:** FPIs are mandated to conduct a comprehensive review of all existing cloud service contracts and SLAs to ensure they align with the minimum requirements outlined in this schedule. Where an existing agreement is found to be non-compliant, the FPI must engage the service provider to renegotiate and

amend the contract accordingly within a transition period not exceeding twelve (12) months from the effective date of this Guideline.

17.4. Roles and Obligations of Cloud Service Providers and Service Integrators

CSPs and SIs are critical to the successful implementation of the Cloud First Principle. As subjects of this Guideline, they have the following obligations:

I. **Certification and Compliance:**
   a. All **CSPs** whose services are used by FPIs must be certified by NITDA.
   b. All **SIs** bidding for projects must be certified by NITDA and listed on the Digital Regulatory Platform. SIs must demonstrate appropriate systems integration capability to qualify for contracts.
   c. A **CSP** acting in the capacity of a Service Integrator for an FPI must be separately certified as an **SI** and is required to comply with all local content and operational obligations applicable to SIs.

II. **Local Content Development:**
   a. All **SIs** must be indigenous companies. They are responsible for providing a detailed local content development plan for job creation and human capital development.
   b. **SIs** must prioritise the use of indigenous CSPs where local capacity exists and meets the technical requirements of the FPI.

III. **Data Protection and Security:**
   a. **CSPs** have a primary obligation to protect the confidentiality, integrity, and availability of their cloud infrastructure ("security *of* the cloud").
   b. **SIs**, by contract, assume a significant portion of the FPI's responsibility for "security *in* the cloud." They are liable for the secure configuration and management of the cloud services they provision.

Any data breach resulting from SI misconfiguration or mismanagement shall render the SI jointly and severally liable with the CSP, unless the breach is demonstrably attributable to one party alone, and must be disclosed immediately to the FPI and NITDA.

IV. **Contractual and SLA Adherence:**

a. **SIs** and **CSPs** must adhere strictly to the terms of their contracts and SLAs with FPIs.
b. SLAs must include provisions for penalties if contractual undertakings are not fulfilled. **SIs** are responsible for managing and enforcing these SLAs on behalf of the FPI.
c. **SIs** must ensure that contracts facilitate data portability and include a clear exit strategy to prevent vendor lock-in.

V. **Cost Optimisation**

a. **SIs** are responsible for designing and managing cloud solutions that are fiscally responsible. They must help the FPI achieve cost-efficiency gains by optimising resource consumption and driving labour efficiency through expert managed services, tooling, and automation, thereby ensuring value for money in all cloud deployments.
b. **SIs** must implement Financial Operations (FinOps) principles, including continuous monitoring of cloud spend, right-sizing of resources to match workload demands, and leveraging cost-saving instruments like reserved instances or savings plans.
c. **SIs** must provide the FPI with transparent, regular reports on cloud usage and costs to prevent budget overruns and identify opportunities for further savings.

VI. **FPI Onboarding and Monitoring:**

a. **SIs** are responsible for the proper onboarding and training of relevant FPI staff on the use and secure

management of the provisioned cloud services, thereby minimising the FPI's operational risk and potential liability.

b. **SIs** must implement systems to monitor for unauthorised access to the FPI's cloud environment and provide formal reports to the FPI and NITDA as required or upon discovery of an incident.

VII. **Capacity Building & Training:**

a. **CSPs**, **SIs**, and **FPIs** shall ensure that their personnel undergo regular capacity-building and certification programmes on cloud governance, data privacy, and cybersecurity. Training shall align with NDPA requirements and ensure staff are equipped to uphold compliance obligations.

18 Schedule C: Cloud Migration and Deployment Framework for FPIs

Purpose

This framework provides FPIs with a structured, mandatory methodology for planning and executing the migration of IT systems, applications, and data to the cloud. It is designed to minimise risk, reduce disruption, and ensure a secure and efficient transition.

18.1. Phased Migration Approach

FPIs shall adopt the following three-stage migration and deployment process:

Stage 1: Select (Assessment and Planning)

I. **Identify and Prioritise Services for Migration:** FPIs shall maintain a living inventory of IT services and applications, updated annually, and prioritise migration candidates based on expected value, readiness, and impact on service delivery.

II. **Conduct Cloud Readiness Assessment:** FPIs must evaluate their internal readiness, including security posture, market availability of suitable services, and the technological lifecycle of existing assets. Assessments must be documented in a Cloud Readiness Report, submitted to NITDA upon request.

III. **Application and Data Classification:** Before migration, all applications and associated data must be classified according to **Schedule A** to determine the appropriate cloud environment and migration strategy (e.g., rehost, refactor, rebuild). FPIs shall not migrate any data classified as Level 4 (Classified) without NITDA's explicit written authorisation, issued in consultation with ONSA.

Stage 2: Provision (Procurement and Integration)

I. **Procure Aligned Services:** All procurements must be conducted exclusively through the Digital Regulatory Platform and comply with **Schedule B's** mandatory

requirements.

II. **Ensure Interoperability:** The new cloud service must be integrated with the FPI's existing IT portfolio in adherence with the Nigerian e-Government Interoperability Framework (Ne-GIF) to avoid data silos. Interoperability testing results shall be documented and retained for audit.

III. **Secure Migration Execution:** Data migration must be conducted using secure methodologies, including end-to-end encryption, integrity checks (e.g., checksums), and comprehensive backups to prevent data loss. All migration events must have rollback procedures tested in advance and logged for accountability.

IV. **Role of Service Integrators:** FPIs shall engage a certified **Service Integrator (SI)** from the Digital Regulatory Platform to lead the technical planning, execution, and management of the migration. The SI is responsible for integrating the chosen CSP services into the FPI's environment securely and efficiently. However, the FPI retains ultimate accountability for its data and overall compliance with this framework.

Stage 3: Manage (Operations and Optimisation)

I. **Shift to Service Management:** Transition the internal IT operational model from managing physical assets to managing cloud services, focusing on performance and user experience.
II. **Upskill Workforce:** Invest in training and certification to equip IT staff with the skills required for cloud architecture, security, and vendor management.
III. **Actively Monitor SLAs:** Continuously monitor CSP performance against the agreed-upon SLA to ensure compliance, address issues proactively, and drive continuous improvement.
IV. **Implement FPI Operational Responsibilities:** The FPI's internal cloud team is responsible for managing its obligations under the Shared Responsibility Model.

This includes, but is not limited to:

a. Configuring and managing all user access through Role-Based Access Controls (RBAC) and the principle of least privilege.
b. Securing applications and workloads deployed on the cloud infrastructure.
c. Managing network controls, firewall configurations, and data encryption within their cloud environment.
d. Monitoring for and responding to security threats within their scope of control.

V. **Manage Data Withdrawal:** Ensure a clear and tested process exists for retrieving and deleting all government and regulated sector data from the CSP's environment upon contract expiration or termination, as defined in the SLA, within the maximum timelines set in Schedule B, section 17.3 (not exceeding 90 days).

19 Schedule D: National Cloud Governance Framework

Purpose

This framework establishes the **Sovereign Cloud Governance Committee (SovGov)**, defining its member bodies, roles, responsibilities, and decision-making authority for overseeing the implementation and enforcement of the National Cloud Computing Guideline. It ensures accountability, inter-agency coordination, and alignment with Nigeria's national objectives.

19.1 Sovereign Cloud Governance Committee

Establishment and Mandate: The Sovereign Cloud Governance Committee (the "Committee") is hereby established as an advisory body responsible for the governance of this Guideline. Its mandate is to ensure a coordinated approach to cloud adoption, enforce compliance with national standards, and steer the strategic evolution of Nigeria's sovereign cloud ecosystem.

Composition of the Committee: The Committee shall comprise representatives from relevant Government institutions, sector regulators, industry and the private sector, with NITDA serving as the Secretariat.

The Terms of Reference (ToR) of the committee shall be developed by NITDA to define the roles and responsibilities of members and ensure effective implementation of the Guideline.

The Committee may invite subject matter experts, representatives of relevant public institutions, industry, academia, development partners, or such other persons as it considers necessary to attend any of its meetings for the purpose of providing technical advice, specialised expertise, or other assistance.

19.2. Data Sovereignty Compliance Mechanisms

To enforce the data sovereignty and security principles of this Guideline, the following compliance mechanisms are hereby established:

I. **Continuous Monitoring:** FPIs are required to utilise tools to continuously monitor their cloud environments

for security misconfigurations and compliance deviations. CSPs must provide transparent access to logs and security dashboards to facilitate this oversight. Logs must be retained for a minimum of 24 months and be available for forensic audit upon request.

II. **Periodic Audits:** NITDA will ensure the compliance of all CSP and SI infrastructure through a **"Trust but Verify"** audit framework. NITDA, or a certified third-party auditor contracted by NITDA, will conduct periodic audits of SIs, CSPs and FPI cloud deployments. These audits will verify adherence to existing regulations, SLA commitments, the Data Classification Framework, security standards, and data hosting requirements. Results may be shared with other relevant oversight authorities for accountability.

III. **CSP and SI Certification Pathway:** NITDA shall manage the certification process for all CSPs and SIs in line with its existing frameworks (NDIAF) and best practices for accrediting IT service providers.

a. **Application:** To be listed on the Digital Regulatory Platform, a CSP must apply to NITDA and submit documentation proving compliance with all standards outlined in the National Cloud Technical Guideline, NDIAF and other forms as established by NITDA.

b. **Vetting and Approval:** NITDA will conduct a technical and security assessment; approval shall be issued by NITDA. Once approved, the CSP will be granted "Pre-approved Status" and listed on the Digital Regulatory Platform.

c. **Continuous Compliance Audit Framework:** NITDA shall establish and maintain a framework of transparent procedures for continuous compliance audits. The Committee is responsible for ensuring these audit procedures remain effective and will periodically update them to align with changes in the global cloud industry and Nigeria's evolving

national interest needs.

d. **Strategic Investment Waiver for Data Localisation:** Based on the recommendation of SovGov, NITDA may grant a temporary waiver for the data localisation requirement to a foreign CSP that demonstrates a concrete and verifiable plan for significant, time-bound investment in local data centre and cloud infrastructure. During the waiver period, which shall be granted at NITDA's discretion and shall not exceed one year at a time, and is renewable once only, the CSP may be accorded the status of an indigenous provider for the purpose of procurement evaluations and listing on the Digital Regulatory Platform. Any provider holding a **provisional indigenous status under Schedule B** must also comply with this waiver framework where hosting is outside Nigeria.

e. **Provisional Certification Pathway:** To further stimulate the local ICT ecosystem and support indigenous innovation, this Guideline establishes a Provisional Certification Pathway. This pathway is designed to foster the development of the local industry by allowing indigenous CSPs, who demonstrate verifiable progress toward meeting full compliance with international standards, to be listed on the Digital Regulatory Platform without encumbrance. Detailed criteria and the 24-month roadmap requirements are set out in Annex D of the National Cloud Technical Guideline.

19.3. The Shared Responsibility Model

All cloud deployments under this Guideline shall operate on a Shared Responsibility Model, which defines the division of liability. The precise delineation of responsibilities under this model is a mandatory component of all Service Level Agreements (SLAs) entered into by FPIs, as stipulated in Schedule B.

I. **The CSP** is responsible for the **security *of* the cloud**.

This includes the physical data centres and the core infrastructure.

II. **The FPI** is ultimately responsible for the **security *in* the cloud**.

III. **The SI**, through its contract with the FPI, takes on the operational management of the FPI's security responsibilities. The SI is directly liable to the FPI for the secure configuration of cloud services, management of access controls, and protection of applications it deploys. The FPI retains final accountability. The specific technical controls SIs are responsible for, including but not limited to identity and access management, use of Multi-Factor Authentication (MFA), password policies, and geolocated access controls, shall be explicitly detailed in the National Cloud Technical Guideline.

19.4. Enforcement and Compliance

NITDA is responsible for the overall enforcement of this Guideline. Any failure by an FPI, a CSP or an SI to comply with the stipulations in this Guideline or its schedules shall be deemed a breach of the NITDA Act, 2007 and subject to sanctions. NITDA, in coordination with the relevant sector regulator, will investigate all reported breaches, conduct a root cause analysis, and determine appropriate sanctions, which may include financial penalties and disqualification from the Digital Regulatory Platform.

19.5. Status of Service Providers

CSPs and SIs are subjects of this governance framework. They are not members of SovGov but are service providers who must operate in full compliance with the regulations, standards, and guidelines enforced by the bodies listed in section 19.1. Their adherence will be monitored through audits, certifications, and the contractual obligations established in **Schedule B**: **Cloud Service Provisioning and Procurement Guidelines for FPIs**.

This Instrument was signed this 4th Day of August 2026

Kashifu Inuwa Abdullahi, *CCIE*
Director-General/CEO
National Information Technology Development Agency