THE FEDERAL REPUBLIC OF NIGERIA 2025

NITDA
National Information Technology Development Agency

NATIONAL CLOUD POLICY

NATIONAL SOVEREIGN CLOUD INITIATIVE

National Cloud Policy 2025 (NCP2025)

National Information Technology Development Agency

S/N	Author	Version No.	Release Date	Change Detail	By Who
1.	TWG	1.0	Sep 2025	First Review	NITDA

Metadata of the Regulation

S/N	Data Element	Value
1.	Title	National Cloud Policy 2025
2.	Short Title	NCP2025
3.	Document Identifier	TBC
4.	Document Version, month, year of release	V 1.0 Oct, 2025
5.	Publisher	NITDA
6.	Type of Regulation Document *(Standard/Policy / Technical Specification / Best Practice / Guideline / Framework / Policy Framework / Procedure)*	Policy
7.	Enforcement Category *(Mandatory / Recommended)*	Mandatory
8.	Owner of approved regulation	NITDA
9.	Target Audience	All Government organisations (including Local, State and Federal Government); ICT Product/Service Providers for public institutions; Cloud Service Providers; Professional Bodies; Development Partners; and General Public.
10.	Copyrights	NITDA
11.	Format	PDF
12.	Subject *(Major area of Standardization)*	Cloud Computing

Table of Contents

Glossary

A. Definitions

For the purpose of this policy, the following definitions shall apply:

Term	Definition
Adequacy / Adequate Protection Standards	The standard of protection required under the NDPA 2023 and any guidance by the NDPC, including jurisdictions formally recognised by NITDA/NDPC as providing equivalent or stronger data protection than Nigeria.
BPP	Bureau of Public Procurement, the primary public procurement regulator under the Public Procurement Act, 2007.
CapEx	Capital Expenditure, meaning upfront investment in fixed IT assets or infrastructure, as opposed to operational subscription models.
Cloud First	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	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)	An entity that offers cloud computing services (IaaS, PaaS, SaaS) and is contractually responsible for service levels and security of those services. A CSP may operate its own infrastructure or use contracted facilities/partners. This includes large-scale providers often referred to as hyperscalers.
Data Breach	Any confirmed or suspected incident leading to the unauthorised access, disclosure, alteration, or destruction of data processed under this Policy.
Data Controller / Processor	As defined by the NDPA 2023; 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	The physical or geographical location of an organisation's data or information.
Data Sharing Agreement (DSA)	A legally binding agreement between FPIs governing the lawful basis, scope, security, and auditability of inter-agency data exchanges, as required under Ne-GIF.
Digital Marketplace	The official government portal for the procurement of pre-approved cloud services, CSPs, Sis, and related offerings for use by FPIs, available at cloudfirst.gov.ng or any successor URL, governed by NITDA rules on listing, suspension, and removal.
Federal Public	Any Ministry, Department, and Agency of the Federal Government of

Institution (FPI)	Nigeria, including any unit that processes government data under mandate or contract.
FinOps	Financial Operations principles applied to cloud cost optimisation, including continuous monitoring, right-sizing, and savings instruments.
Hybrid Cloud	A deployment model combining private and public cloud infrastructure, where sensitive data may be kept in private environments and other workloads in public or community clouds.
IaaS	Infrastructure-as-a-Service, a cloud service model providing virtualised computing resources such as servers, storage, and networking.
Indigenous Provider / Indigenous Cloud Service Providers / Indigenous Service Integrator	A CSP or SI incorporated in Nigeria and certified by NITDA as compliant with local content requirements. Foreign CSPs may be granted provisional indigenous status under strategic investment rules.
Latency / Access Benchmarks	National or internationally recognised standards for network speed and reliability required to ensure government services hosted in the cloud remain accessible to end-users.
MLAT	Mutual Legal Assistance Treaty, an international agreement establishing lawful frameworks for cross-border government-to-government data access requests.
NDPA	Nigeria Data Protection Act, 2023, the national law governing personal data processing and cross-border transfers.
NDPC	Nigeria Data Protection Commission, the statutory body mandated to enforce NDPA compliance.
Ne-GIF	Nigerian e-Government Interoperability Framework, the federal framework for ensuring cross-agency systems can securely exchange data.
NITDA	National Information Technology Development Agency, the chair of SovGov and lead coordinating body for implementation of this Policy.
ONSA	Office of the National Security Adviser, the lead authority on matters of national security, particularly Level 4 classified data
OpEx	Operational Expenditure, meaning ongoing subscription-based or pay-as-you-go IT costs as opposed to upfront CapEx investments.
PaaS	Platform-as-a-Service, a cloud service model providing platforms and runtime environments for developing, testing, and deploying applications.
PIA / DPIA	Privacy Impact Assessment / Data Protection Impact Assessment, required assessments under the NDPA for new systems processing personal data.
PPP	Public-Private Partnership, a contractual collaboration between government and private entities for infrastructure or service delivery.
RBAC	Role-Based Access Control, a security principle requiring that users be

	granted only the access rights strictly necessary to perform their duties.
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss measured in time (e.g., last 4 hours of data).
Recovery Time Objective (RTO)	The maximum acceptable downtime after a disruption before services must be restored.
SaaS	Software-as-a-Service, a cloud service model where software applications are delivered over the internet on a subscription basis.
Schedule A	National Data Classification Framework (part of this Policy).
Schedule B	Cloud Service Provisioning and Procurement Guidelines (part of this Policy).
Schedule C	Cloud Migration and Deployment Framework (part of this Policy).
Schedule D	National Cloud Governance Framework (part of this Policy).
Service Integrator (SI)	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 the primary provisioning entities for government services under this policy.
Service Level Agreement (SLA)	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	The framework, as defined in Schedule D, that delineates responsibilities of CSPs, FPIs, and Sis.
Sovereign Cloud Governance Committee (SovGov)	The inter-agency steering committee established to manage the use of cloud services by FPIs and oversee compliance for government cloud adoption.
Strategic Investment Waiver	A temporary localisation waiver granted by NITDA/SovGov to a foreign CSP that commits to verifiable, time-bound investments in Nigerian cloud infrastructure.
Vendor Lock-in	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.

B. Interpretation

1. Status of Schedules

The Schedules (A - D) form an integral part of this Policy 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 Policy shall have the meanings assigned to them in the Glossary unless the context otherwise requires. Where a term is defined in both this Policy 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 Policy 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 NDPA 2023, Public Procurement Act 2007, and Cybercrimes (Amendment) Act 2024) shall prevail over this Policy;
(b) This Policy and its Schedules shall prevail over any conflicting internal policy, contract, or practice of an FPI, CSP, or SI, unless expressly exempted by SovGov;
(c) SovGov's directives, issued under delegated authority, are binding and prevail over conflicting institutional practices.

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."

Executive Summary

The Nigerian Cloud Policy 2025 (NCP2025) establishes a "Cloud First" directive to accelerate the nation's digital transformation, providing a comprehensive framework to ensure the adoption of cloud computing is secure, sovereign, and economically beneficial. This Policy affirms Nigeria's sovereign ownership over its data assets, by mandating a national data classification framework and local data residency requirements, while establishing regulatory certainty to attract and safeguard strategic investment.

A **Sovereign Cloud Governance Committee** is hereby established to provide unified oversight, ensuring that cloud adoption aligns with national priorities. The Policy formalises the designation of indigenous **Service Integrators (SIs)** as the primary entities for provisioning government cloud services, thereby entrenching local content obligations as a central pillar of Nigeria's ICT strategy.

To balance security and accountability, the NCP2025 embeds a **Shared Responsibility Model**, clearly defining the distinct liabilities of Cloud Service Providers (CSPs), Service Integrators, and Federal Public Institutions (FPIs). Furthermore, to facilitate participation by global hyperscalers, the Policy introduces a **Strategic Investment Waiver**, providing a transparent, incentive-based pathway for market entry contingent upon verifiable commitments to in-country infrastructure development and capacity building.

By promoting indigenous ICT products and pre-approved cloud services through a certified Digital Marketplace (www.cloudfirst.gov.ng), the Policy aims to stimulate local innovation, drive GDP growth, and ensure that Nigeria's digital future remains both resilient and self-reliant.

1.0 Introduction

The global economy is increasingly reliant on Information and Communication Technology (ICT), making the availability and accessibility of computing resources critical for sustainable development. Nigeria's national economic strategies, including the Economic Recovery and Growth Plan (ERGP) identifies ICT as a primary enabler of digital-led growth. However, challenges such as high upfront and recurring cost of IT investments, inefficient infrastructure, and a fragmented regulatory environment hinder progress.

This Policy addresses these gaps by establishing a unified framework for cloud adoption, drawing upon and superseding the 2019 Nigeria Cloud Computing Policy and aligning with the Nigeria Data Protection Act (NDPA) 2023. While this Policy's primary mandate applies to Federal Public Institutions (FPIs), its principles are founded on the NDPA 2023, which has extraterritorial scope and applicability to any entity processing the personal data of Nigerian citizens, thereby reinforcing a uniform national standard for data governance and sovereignity.

2.0 Applicability

2.1 Scope of Services

This Policy governs the procurement, deployment, operation, and support of all cloud services and infrastructure used by covered entities, including new acquisitions and existing deployments. All existing cloud deployments must be reviewed and brought into compliance within a transition period not exceeding twelve (12) months from the effective date of this Policy, as determined by NITDA through implementation guidance.

2.1 Entities Covered

This Policy and the associated schedules and technical documents shall apply to the following entities:

- **Federal Government**: This Policy is **mandatory** for all Federal Public Institutions (FPIs) and all Federal Government-owned companies.

- **State and Local Governments**: While this is a federal policy, adoption is **strongly encouraged** for State and Local Governments to foster a unified national digital framework and enhance interoperability across all tiers of government.

- **Contractors, Partners, and Service Providers**: This Policy applies to Cloud Service Providers (CSPs), Service Integrators (SIs), and other private-sector partners (including Public-Private Partnerships entities) engaged by FPIs. Compliance shall be enforced through mandatory contractual clauses in all agreements with FPIs, making adherence to this Policy a condition of award and continuing performance. Such obligations shall flow down contractually to all subcontractors and sub-processors engaged in the delivery of services to FPIs.

- **Designated Private Sector Data**: The mandates of this Policy, particularly the Data Residency and security requirements outlined in **Schedule A**, apply to any private sector entity that processes data designated by NITDA and the Office of the National Security Adviser (ONSA) as being of strategic national interest.

3.0 Objectives

The primary goal of this Policy 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.

Specific objectives include:

- To stimulate the development and consumption of high-quality ICT products and services from indigenous companies.
- To create an enabling environment that attracts hyperscaler and data center investments through clear, stable regulations and incentives.
- To ensure the security, transparency, and sovereignty of Nigeria's cloud ecosystem in alignment with national and international standards.
- To provide a framework for compliance with Presidential Executive Orders 003 (2017) and 005 (2018) on local content and the promotion of Nigerian enterprise.
- 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.

4.0 Core Policy Directives

4.1 Cloud First Principle

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.

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 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 Document 2025**.

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.

4.2 Data Classification and Transfers:

All personal data processing must adhere strictly to the Nigeria Data Protection Act 2023 (NDPA).

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

Data transfers across borders are permissible only when fully compliant with the NDPA and this Policy'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 Policy 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. The specific guidelines governing these operational transfers are detailed in the **National Cloud Technical Document 2025**.

4.3 Data Sovereignty and Residency:

Nigeria asserts its sovereign right to govern data processed and stored within its territory. All sovereign data classified as Level 3 and 4, as defined and categorised in **Schedule A: National Data Classification Framework**, shall be hosted exclusively within Nigeria, subject to temporary waivers as provide 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 as part of a strategic investment initiative, as detailed in Schedule D, Section 3.0.

This directive is consistent with Section 13.1 of the Guidelines for Nigerian Content Development in ICT (2019), which mandates local hosting of sovereign data.

4.4 Future-Proofing and Scalability

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

- **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.

- **Future-Proofing**: To avoid technological obsolescence and prevent vendor lock-in, the Policy 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.

The responsibility for updating the technical standards accompanying this policy is placed **NITDA**, acting under the strategic oversight of the **SovGov**.

4.5 International Cooperation and Alignment

This Policy 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 **SovGov**. 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.

5.0 Security, Privacy, and Risk Management

5.1 Data Privacy and Protection

All 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.

5.2 Risk Management Framework

FPIs 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 Document 2025**.

5.3 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) hall 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 Document 2025.**

5.4 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.

5.5 Intra-Governmental Data Access

Access to data held by one FPI by another shall be prohibited unless expressly authorised under law to protect data integrity and privacy in accordance with the NDPA 2023. However, to facilitate government operations, two distinct pathways for data sharing are established:

1. **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.

2. **Sensitive and Ad-Hoc Sharing:** For any ad-hoc or sensitive data access requests that fall outside the scope of an established DSA, a court order or explicit statutory authorisation shall be required.

5.6 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 NITDA or a SovGov-certified auditor.

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

6.0 Service and Operational Principles

6.1 Access and Connectivity Standards

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

6.2 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.

6.3 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 Document 2025, to ensure seamless integration and data portability between government systems.

6.4 Mandate for Service Level Agreements (SLAs)

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

7.0 Governance and Implementation

7.1 National Cloud Governance Framework

A **Sovereign Cloud Governance Committee (SovGov)** is hereby established to oversee the implementation and enforcement of this Policy. NITDA shall serve as the lead implementing and

coordinating authority for the governance of this Policy, 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.

7.2 Implementation Guidelines & Compliance Support

To ensure the successful and consistent application of this Policy across all Federal Public Institutions (FPIs) and other relevant stakeholders, the Sovereign Cloud Governance Committee (SovGov) is hereby mandated to develop, maintain, and periodically update a suite of implementation guidelines and support materials.

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

- A detailed Data Classification and Residency Implementation Guideline.
- Technical best practices for cloud migration and deployment.
- Security and risk management protocols.
- Templates for procurement and Service Level Agreements (SLAs).
- A defined grace period for FPIs to build capacity, inventory their data assets and develop phased migration plans for non-compliant services.

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 Policy's effective date, with other support materials issued thereafter on a rolling basis. These and other resources shall be made readily available via the Digital Marketplace.

7.3 Financial Operations (FinOps) and Cost Management

FPIs shall transition from capital expenditure (CapEx) to operational expenditure (OpEx) models for IT procurement. Cloud contracts must be structured on a "pay as you go" basis to optimize costs.

To leverage economies of scale, the Sovereign Cloud Governance Committee (as defined in **Schedule D**), shall have authority to aggregate cloud usage data across FPIs through the Digital Marketplace (www.cloudfirst.gov.ng), to:

- Negotiate whole-of-government purchase agreements;
- Drive further cost savings; and
- Disseminate best practices across all levels of government (Federal, State and Local).

7.4 Environmental Sustainability

This Policy promotes the adoption of green cloud technologies. FPIs are encouraged to procure services from CSPs that utilise energy-efficient data centers and renewable energy solutions to reduce the national carbon footprint.

8.0 Compliance and Enforcement

8.1 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 Document 2025**.

8.2 Penalties and Sanctions

Any breach of the guidelines within this Policy will be deemed a breach of the NITDA Act of 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 compromise the following graduated measures:

1. Administrative Actions: For minor administrative or procedural issues, NITDA may issue a formal warning and require the submission of a corrective action plan.

2. Contractual and Certification Actions: For more significant operational or compliance failures, NITDA may apply administrative fines, temporarily suspend a provider's services from the Digital Marketplace, and/or mandate a formal recertification audit.

3. Statutory Penalties: The administrative and contractual sanctions under this Policy 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.

Schedules to NCP2025

Schedule A: National Data Classification Framework

1.0 Purpose

This framework is built on the principle that data is a critical national asset. Compliance with this Policy requires that all Federal Public Institutions (FPIs) shall develop the capacity to effectively govern their data. This process shall begin with an inventory of all data assets to understand their scope, value, and sensitivity.

Once an FPI has a clear understanding of the data it holds, this framework establishes a mandatory classification system to ensure that government and citizen data are managed, stored, and protected according to their sensitivity, criticality, and risk. It establishes a consistent methodology for risk management, ensures compliance with the Nigeria Data Protection Act (NDPA) 2023, and serves as the foundation for enforcing Nigeria's data sovereignty and residency requirements.

2.0 Data Classification Levels

All government, citizen, and corporate data handled by FPIs must be classified into the following levels, organised by sensitivity. This classificaton also applies to public interest and other non-personal data categories not specifically addressed by the NDPA.

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 records 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	Data shall be primarily hosted in a private or secure hybrid cloud within Nigeria's territorial boundary. Cross-border transfer is permissible only under conditions expressly provided in the NDPA	Mandatory
Level 2	Sensitive	Personal financial, health and social information	Data may be hosted in a cloud environment within Nigeria's territorial boundary	Highly Recommended

			or, where legally permissible, abroad. Cross-border hosting shall be subject to explicit consent or other legal basis under the NDPA, provided that the hosting jurisdiction maintains adequate protection standards and meets national or internationally recognised low 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

LEVEL 4 - CLASSIFIED

- **National Security Data**
  - **Sensitivity Level:** Classified
  - **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.
  - **Examples:** Military intelligence, law enforcement investigation data, critical national infrastructure schematics, strategic national secrets, and diplomatic communications of a sensitive nature.
  - **Hosting Requirement:** Data shall reside exclusively on-premises within the FPI, in a collocated private data centre, or in a government-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 Document 2025**.
  - **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.

LEVEL 3 - HIGHLY SENSITIVE

- **Public Sensitive Data**
  - **Sensitivity Level:** High
  - **Description:** Public sector data which, if compromised, could significantly affect national security, or the economy.
  - **Examples:** Critical economic data, strategic policy documents, and regulated

industry information which, if prematurely disclosed, may constitute market manipulation, confer unfair competitive advantage, or disruption orderly governance.
    - **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 is permissible only under NDPA-compliant conditions and subject to NITDA approval, where applicable.
    - **Data Retention & Erasure:** Data shall not be retained beyond what is strictly for its lawful purpose. Retention policies shall be documented, clearly defined and auditable. Erasure shall be effected using secure and verifiable data sanitisation methods.

- **Corporate Confidential Data**
    - **Sensitivity Level:** High
    - **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.
    - **Examples:** Proprietary industry data, sensitive financial market information, data from PPPs, data from CNII, and trade secrets vital to the national economy.
    - **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.
    - **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.

LEVEL 2 - SENSITIVE

- **Private Sensitive Data or Confidential**
    - **Sensitivity Level:** Moderate
    - **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.
    - **Examples:** Sensitive personal data as defined by the NDPA, confidential reports, and internal records of public institutions or SMEs.
    - **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.
    - **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.

- **Private Insensitive Data**
    - **Sensitivity Level:** Moderate
    - **Description:** Personal data not classified as sensitive but still subject to NDPA protections, including non-sensitive data held by public institutions and SMEs.
    - **Examples:** Basic personal identification information, non-sensitive records held by public institutions, and general operational data of SMEs.
    - **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.
    - **Data Retention & Erasure:** Retention policies must comply with the NDPA. Standard secure deletion practices are required upon the expiration of the retention period.

LEVEL 1 - OPEN

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

- **Corporate Non-Confidential Data**
    - **Sensitivity Level:** Low
    - **Description:** General non-confidential business information from industry, private, or public sector entities that is not confidential and is intended for public dissemination.
    - **Examples:** Corporate annual reports, marketing materials, public-facing product information.
    - **Hosting Requirement:** Data may be hosted in a public cloud environment that complies with national or internationally recognised information standards.
    - **Data Retention & Erasure:** Retention is determined by the business relevance of the data. Standard deletion practices shall apply where erasure is required.

3.0 Responsibilities of FPIs, CSPs and SIs

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 policy and its schedules.

3.1 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 policy implementation outlined in **Schedule D**, FPIs must:

- **Data Classification:** Inventory and classify all data assets in accordance with the mandatory classification framework in **Schedule A: National Data Classification Framework.** FPIs shall establish retention schedules with maximum permissible timeframes for each classification level, except where overridden by statutory or national security requirements.
- **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.
- **Procurement and Contracts:** Ensure all procurement of cloud services adheres strictly to the guidelines in **Schedule B: Cloud Procurement Framework**, including all contractual and SLA requirements.
- **Data Sharing for Policy Oversight:** FPIs are mandated to share necessary operational, consumption, and compliance data with SovGov and NITDA upon request. This data sharing is required to enable effective monitoring and tracking of this policy's implementation and to allow NITDA to identify opportunities for shared services and other beneficial cross-government solutions.

3.2 Responsibilities of Cloud Service Providers (CSPs)

All CSPs handling government data are contractually obligated to adhere to this Policy. They must:

- **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 Document 2025**.
- **Enable FPI Compliance:** Provide FPIs with the necessary service configurations and management tools to allow them to manage their data according to its classification.
- **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.

3.3 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 Policy. They must:

- **Adhere to Classification:** Implement and manage cloud environments in strict accordance with the FPI’s data classification decisions.

- **Uphold Shared Responsibility:** Fulfill 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.
- **Maintain Technical Standards:** Ensure all configurations and deployments comply with the minimum standards outlined in the **National Cloud Technical Document 2025**.

Schedule B: Cloud Service Provisioning and Procurement Guidelines for FPIs

1.0 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" policy, and prioritisation of local content.

2.0 The Digital Marketplace

The Digital Marketplace (www.cloudfirst.gov.ng), managed jointly by NITDA and the Bureau of Public Procurement (BPP), is the mandatory and exclusive portal for the procurement of all cloud services by Federal Public Institutions (FPIs).

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

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

3. **Publication of Marketplace Listing Process:** The Sovereign Cloud Governance Committee (SovGov) 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 Marketplace.

4. This complete directive shall be made publicly available on the official NITDA website and the marketplace portal (www.cloudfirst.gov.ng) no later than **three (3) months** from the effective date of this Policy.

3.0 Procurement Process

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

2. **Marketplace Review and Sourcing:** Procurement of cloud services must be conducted through the government's official digital marketplace for cloud providers: **cloudfirst.gov.ng**. This portal, managed by NITDA and the BPP, will contain a list of pre-approved CSPs and their service offerings, enabling transparent comparison.

3. **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**.

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

   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 center infrastructure. Criteria for what constitutes a “suitable investment” shall be objective, measurable, and published by SovGov, 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 4.0 (4).** For guidance, a framework for evaluating strategic investments is provided in **Annex H of the National Cloud Technical Document 2025**.

   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 Document** 2025 and verified during their certification for the Digital Marketplace.

5. **Contracting and Financial Model:** All cloud service contracts shall be structured on a "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 requirement in Scetion 4.0.

6. **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 administered by SovGov.

4.0 Minimum SLA Requirements

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

- **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).

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

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

- **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.

- **Penalties for Non-Performance:** A clear penalty clause for any failure to meet agreed-upon service levels. While this Policy 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 the **National Cloud Technical Document 2025**.

- **Data Ownership and Exit Strategy:** A clause affirming that the FPI retains full ownership of its data at all times. Exit strategy provisions must specify maximum timelines (not exceeding 90 days) for the secure and complete repatriation, transfer, and/or deletion of all government data upon contract expiration or termination.

- **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).

- **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 commencement of this Policy, as defined by SovGov in its implementation guidance.

5.0 Roles and Obligations of Cloud Service Providers and Service Integrators

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

1. **Certification and Compliance:**
    - All **CSPs** whose services are used by FPIs must be certified by NITDA.
    - All **SIs** bidding for government projects must be certified by NITDA and listed on the Digital Marketplace. SIs must demonstrate appropriate systems integration capability to qualify for contracts.
    - 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.

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

3. **Data Protection and Security:**
    - **CSPs** have a primary obligation to protect the confidentiality, integrity, and availability of their cloud infrastructure ("security *of* the cloud").
    - **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.

4. **Contractual and SLA Adherence:**
    - **SIs** and **CSPs** must adhere strictly to the terms of their contracts and SLAs with FPIs.
    - 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.

- **SIs** must ensure that contracts facilitate data portability and include a clear exit strategy to prevent vendor lock-in.

5. **Cost Optimization**
    - **SIs** are responsible for designing and managing cloud solutions that are fiscally responsible. They must help the FPI achieve cost-efficiency gains by optimizing resource consumption and driving labor efficiency through expert managed services, tooling, and automation, thereby ensuring value for money in all cloud deployments.
    - **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.
    - **SIs** must provide the FPI with transparent, regular reports on cloud usage and costs to prevent budget overruns and identify opportunities for further savings.

6. **FPI Onboarding and Monitoring:**
    - **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 minimizing the FPI's operational risk and potential liability.
    - **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.

7. **Capacity Building & Training:**
    - **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.

Schedule C: Cloud Migration and Deployment Framework for FPIs

1.0 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.

2.0 Phased Migration Approach

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

Stage 1: Select (Assessment and Planning)

1. **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.

2. **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.

3. **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 "Confidential – National Security" without SovGov's explicit written authorisation.

Stage 2: Provision (Procurement and Integration)

1. **Procure Aligned Services:** All procurements must be conducted exclusively through the Digital Marketplace and comply with **Schedule B's** mandatory requirements.

2. **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.

3. **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.

4. **Role of Service Integrators:** FPIs shall engage a certified **Service Integrator (SI)** from the Digital Marketplace 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)

1. **Shift to Service Management:** Transition the internal IT operational model from managing physical assets to managing cloud services, focusing on performance and user experience.
2. **Upskill Workforce:** Invest in training and certification to equip IT staff with the skills required for cloud architecture, security, and vendor management.
3. **Actively Monitor SLAs:** Continuously monitor CSP performance against the agreed-upon SLA to ensure compliance, address issues proactively, and drive continuous improvement.
4. **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.
5. **Manage Data Withdrawal:** Ensure a clear and tested process exists for retrieving and deleting all government 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 4.0 (not exceeding 90 days).

Schedule D: National Cloud Governance Framework

1.0 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 Policy. It ensures accountability, inter-agency coordination, and alignment with Nigeria's national objectives.

2.0 Sovereign Cloud Governance Committee

2.1 Establishment and Mandate: The Sovereign Cloud Governance Committee (the "Committee") is hereby established as the primary body responsible for the governance of this Policy. Its mandate is to ensure a coordinated, whole-of-government approach to cloud adoption, enforce compliance with national standards, and steer the strategic evolution of Nigeria's sovereign cloud ecosystem. The Committee shall have delegated statutory authority to issue binding directives to FPIs, CSPs, and SIs under this Policy.

2.2 Composition of the Committee: The Committee shall be composed of representatives from the following member organisations. The roles and responsibilities of each member body are set out in Section 3.0 below.

3.0 Governance Bodies and Roles

The roles and responsibilities of the Committee's member organisations shall be as follows:

- **National Information Technology Development Agency (NITDA)**
  - **Role:** Chair and lead coordinating body of the Committee.
  - **Responsibilities:**
    - Drive and monitor government-wide cloud adoption.
    - Establish a baseline of current cloud adoption across all FPIs and implement a monitoring and evaluation framework to report on progress towards this policy's adoption targets.
    - Develop, issue, and periodically review all technical standards, guidelines, and annexes related to this policy.
    - Co-manage the Digital Marketplace: www.cloudfirst.gov.ng with the BPP and certify CSPs for public sector use.
    - Conduct audits and enforce compliance in collaboration with the NDPC. NITDA shall also publish annual compliance audit reports to promote transparency and accountability.
    - Conducts the certification of CSPs/SIs and makes recommendations for final approval by the Committee.

- **Bureau of Public Procurement (BPP):**
  - **Role:** Member of the Committee and the primary public procurement regulator.

- **Responsibilities:**
  - Develop and operationalise government-wide procurement regulations and frameworks for cloud services in consultation with NITDA.
  - Co-manage the Digital Marketplace to ensure transparent and competitive procurement.

- **Office of the National Security Adviser (ONSA)**
  - **Role:** Member of the Committee and the lead authority on matters of national security.
  - **Responsibilities:**
    - Monitor operational security issues related to the cloud ecosystem.
    - Define and audit the specific security requirements for hosting Level 4 (Classified / National Security) data.
    - ONSA shall issue minimum baseline security controls for Level 4 hosting environments, updated annually.

- **Nigeria Data Protection Commission (NDPC)**
  - **Role:** Member of the Committee and the independent authority for data protection.
  - **Responsibilities:**
    - Ensure all cloud deployments and data processing activities comply with the NDPA 2023.
    - Investigate data breaches and enforce penalties for non-compliance with NDPA. NDPC may sanction CSPs/SIs directly, without prejudice to NITDA's parallel enforcement powers.

- **Office of the Secretary to the Government of the Federation (OSGF)**
  - **Role:** Member of the Committee responsible for strategic policy alignment.
  - **Responsibilities:**
    - Ensure the National Cloud Policy aligns with the broader strategic objectives and priorities of the Federal Government.
    - Facilitate inter-ministerial coordination to remove bureaucratic obstacles to cloud adoption.
    - Shall coordinate with Ministry of Finance to ensure budgetary allocations reflect cloud adoption priorities.

- **Office of the Head of the Civil Service of the Federation (OHCSF)**
  - **Role:** Member of the Committee responsible for public service capacity and change management.
  - **Responsibilities:**
    - Lead the change management and capacity-building initiatives required for the civil service to effectively adopt cloud technologies.
    - Develop skills frameworks and training programs related to cloud computing for civil servants.
    - Shall coordinate with Ministry of Finance to ensure budgetary allocations

reflect cloud adoption priorities.

- **Federal Public Institutions (FPIs)**
    - **Role:** The primary implementers of this Policy, subject to the oversight of the Committee.
    - **Responsibilities:**
        - Appoint an internal cloud leader or team to audit data assets and oversee cloud transformation.
        - Develop an internal cloud migration roadmap for existing services in line with **Schedule C**: **Cloud Migration and Deployment Framework for FPIs.**
        - Ensure all cloud services are procured and managed in full compliance with this policy and its schedules.
        - Maintain records of existing cloud services
        - Report on progress and compliance to NITDA as required.

- **Private Sector, Academia and Civil Society Representatives:**
    - **Role:** Non-voting advisory members representing the local ICT industry and end-users within the Committee.
    - **Responsibilities:**
        - Provide industry expertise and insights from key ecosystem players, including Cloud Service Providers (CSPs), Service Integrators (SIs), and other companies involved in the establishment and running of Data Centers.
        - Represent academic and research institutions to create a link between national cloud adoption, local research and development (R&D), and the workforce pipeline.
        - Contribute civil society perspectives on issues such as digital rights, data privacy, and consumer advocacy.
        - Participate in all policy consultations but must abstain from voting on enforcement, procurement, or certification matters to avoid any conflict of interest.
    - **Term of Membership:** Representatives are appointed as individuals and shall serve a single, non-renewable term of three (3) years. This ensures a regular rotation of industry perspectives on the Committee.

4.0 Data Sovereignty Compliance Mechanisms

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

- **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.

- **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.

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

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

    2. **Vetting and Approval:** NITDA will conduct a technical and security assessment; approval shall be issued by SovGov upon NITDA's sucessful verification. Once approved, the CSP will be granted "Pre-approved Status" and listed on the Digital Marketplace.

    3. **Continuous Compliance Audit Framework:** SovGov 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.

    4. **Strategic Investment Waiver for Data Localisation:** 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 center infrastructure. During the waiver period, which shall be granted at NITDA's discretion and should not exceed one year at a time, and is renewable a maximum of three times, the CSP may be accorded the status of an indigenous provider for the purpose of procurement evaluations and listing in the Digital Marketplace. Any provider holding a **provisional indigenous status under Schedule B** must also comply with this waiver framework where hosting is outside Nigeria.

    5. **Provisional Certification Pathway:** To further stimulate the local ICT ecosystem and support indigenous innovation, this policy 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 Marketplace without encumbrance.

5.0 The Shared Responsibility Model

All cloud deployments under this Policy 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.

- **The CSP** is responsible for the **security *of* the cloud**. This includes the physical data centers and the core infrastructure.
- **The FPI** is ultimately responsible for the **security *in* the cloud**.
- **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 Document.

6.0 Enforcement and Compliance

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

7.0 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 3.0. Their adherence will be monitored through audits, certifications, and the contractual obligations established in **Schedule B**: **Cloud Service Provisioning and Procurement Guidelines for FPIs**.