THE FEDERAL REPUBLIC OF NIGERIA 2025

NATIONAL CLOUD TECHNICAL DOCUMENT V1.0

DRAFT

NATIONAL SOVEREIGN CLOUD INITIATIVE

NITDA
National Information Technology Development Agency

National Cloud Technical Document

v1.0

DRAFT

1.0 Executive Summary

This document provides the detailed technical and operational standards required to implement the National Cloud Policy 2025 (NCP2025). It serves as a practical guide for Federal Public Institutions (FPIs), Cloud Service Providers (CSPs), System Integrators (SIs) and other stakeholders, outlining the mandatory requirements for procuring, deploying, and managing cloud services securely and efficiently. The guidelines cover procurement models, security operations, migration methodologies, and the compliance framework needed to ensure Nigeria's sovereign cloud ecosystem is resilient, interoperable, and aligned with global best practices.

2.0 Introduction and Scope

2.1 Purpose of Technical Guidelines

- These guidelines translate the high-level principles of the NCP2025 into actionable technical requirements. They are designed to ensure the secure, scalable, and sustainable deployment of cloud infrastructure in Nigeria.

2.2 Applicability

- The standards herein apply to all new and existing cloud services and infrastructure used by FPIs. This includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) deployments.

2.3 Governing Instruments

- The technical standards and operational mandates within this document are designed to ensure compliance with a unified set of national legal and regulatory frameworks. All FPIs, CSPs, and SIs must ensure their cloud procurement, deployment, and management activities adhere to the following key instruments:
    - The National Cloud Policy 2025 (NCP2025) - The accompanying policy.
    - The Nigeria Data Protection Act (NDP Act) 2023
    - The Guidelines for Nigerian Content Development in ICT
    - The NITDA IT Project Clearance Regulation
    - The Public Procurement Act
    - The Cybercrimes (Amendment) Act 2024

DRAFT

3.0 Objectives

The National Cloud Technical Document aims to provide a clear, unified, and enforceable set of standards for the deployment and operation of sovereign cloud infrastructure in Nigeria.

3.1 To Standardize Technical and Operational Requirements

- This document establishes in-country data center deployment standards aligned with national security, scalability, and sustainability requirements. It provides clarity on the technical specifications for project design and public tenders, covering physical infrastructure, network, compute, and storage. It also includes guidelines for energy-efficient design to reduce carbon footprint and operational costs.

3.2 To Define Best Practices for a Secure and Resilient Cloud Ecosystem

- It defines best practices for cybersecurity, interoperability, and data portability across all cloud platforms. The document incorporates recognition of global security standards and defines clear metrics for availability, resilience, and disaster recovery to ensure the protection of government data and the continuity of digital services.

3.3 To Stimulate Investment and Local Innovation

- By creating a clear and stable technical environment, the document aims to stimulate targeted investment and the development of compatible services for the Nigerian market. It provides a predictable framework that helps attract global hyperscalers while encouraging local partnerships and fostering a competitive market for Nigerian Cloud Service Providers (CSPs.

3.4 To Establish a Unified Compliance Framework

- The document develops a unified compliance and reporting framework for CSPs to ensure adherence to both national and international standards. This includes designing a template for periodic infrastructure status reports and recommending monitoring tools, audit protocols, and certification pathways to enforce compliance effectively.

4.0 Procurement and Service Management

4.1 Sourcing Cloud Services

- FPIs can source services from public, private, or hybrid cloud models, depending on the data classification and business need. Procurement must prioritize local content and

DRAFT

indigenous CSPs in line with the Guidelines for Nigerian Content Development in ICT.

- The "Cloud First" directive requires a thorough evaluation of the best execution venue for each government workload, considering factors such as cost, performance, security, and data sovereignty. For predictable, long-term workloads, FPIs and their SIs must conduct a Total Cost of Ownership (TCO) analysis to determine if a managed private or hybrid cloud model offers better economic value and control than a purely public cloud solution.

4.2 Recognized Deployment Models and Standards

- **4.2.1 Adherence to International and National Standards:** To ensure interoperability, security, and trust, all cloud services procured by FPIs must align with recognized international standards. This policy mandates adherence to the following as a baseline:
    - ISO/IEC 17203: for workload portability and the prevention of vendor lock-in (Open Virtualization Format).
    - ISO/IEC 27017: for a code of practice on information security controls for cloud services .
    - ISO/IEC 27018: for a code of practice on the protection of Personally Identifiable Information (PII) in public clouds .
    - ISO/IEC 19086: for a standardized framework on Cloud Service Level Agreements (SLAs) .
    - Cloud Security Alliance (CSA) STAR Certification (Level 1 minimum)
    - Service Organization Control (SOC) 2 Type II Attestation Report

  While adherence to these global standards is the ultimate goal for ensuring competitiveness and interoperability, this policy also strongly encourages the development of equivalent national standards. This approach is intended to build local expertise, foster a domestic certification ecosystem, and ensure that standards are precisely tailored to Nigeria's unique regulatory and operational context. Indigenous providers may demonstrate compliance through these recognized national standards as they become available.

- **4.2.2 Cloud Service Models (IaaS, PaaS, SaaS, FaaS):** FPIs, working with SIs, shall select the cloud service model that best fits their specific technical requirements and operational needs. The following models are recognized by this policy:
    - **Infrastructure as a Service (IaaS):** For foundational compute, storage, and networking resources.
    - **Platform as a Service (PaaS):** For application development and deployment environments.
    - **Software as a Service (SaaS):** For pre-built, ready-to-use software applications.
    - **Functions as a Service (FaaS) / Serverless:** For event-driven applications where infrastructure management is fully abstracted.The choice of service model must be based on a thorough analysis of the FPI's needs and guided by a fiscally

DRAFT

responsible approach that optimizes public expenditure. While public cloud (IaaS, PaaS) is suitable for workloads with variable demand, FPIs should consider managed private or hybrid cloud models for stable, high-utilization applications, as these can offer significant cost savings and greater control over the long term. The Sovereign Cloud Governance Committee (SovGov) reserves the right to issue updated recommendations on the appropriate use of these models. Furthermore, NITDA may provide guidance to FPIs on the choice of model for specific projects as part of its routine IT project clearance process to ensure alignment with national strategic objectives.

- **4.2.3 Deployment Model Use Cases:** FPIs, in consultation with their SIs, shall select a deployment model based on the data classification and specific use case. The following table provides the recognized models and their primary preferred applications:

Primary Use Case	**Preferred Deployment Model**	**Remarks**
Non-sensitive workloads and citizen-facing services (Level 1 & 2 Data).	**Public Cloud**	Providers must be certified and listed on the Digital Marketplace.
Sensitive and classified government data (Level 3 & 4 Data).	**Private Cloud**	Must be hosted in-country, with a strong preference for indigenous CSPs.
Workloads requiring a mix of security levels or inter-agency integration.	**Hybrid Cloud**	Secure orchestration and data flow between environments is mandatory.
Shared services and platforms used by multiple FPIs.	**Community Cloud**	Must be hosted in-country and may be co-managed by the participating FPIs or a lead agency.

4.3 Technical Requirements for Service Level

DRAFT

Agreements (SLAs)

- **4.3.1 Availability and Support Requirements:** SLAs must meet the following minimum tiered availability and support requirements, which apply 24 hours a day, 7 days a week (24x7). The requirements are linked to the National Data Classification Framework:
    - For services hosting **Level 4 and Level 3 data:**
        - Minimum Availability (Uptime): **99.99%**
        - Critical Incident Support Response Time: **< 15 minutes**
        - Critical Incident Support Resolution Time: **< 4 hours**
    - For services hosting **Level 2 data:**
        - Minimum Availability (Uptime): **99.95%**
        - Critical Incident Support Response Time: **< 1 hour**
        - Critical Incident Support Resolution Time: **< 8 hours**
    - For services hosting Level 1 data:
        - Minimum Availability (Uptime): **99.9%**
        - Support Response Time: **< 4 business hours (during standard Nigerian working hours)**
        - Support Resolution Time: **Best effort, with a target of < 24 business hours**
- **4.3.2 Network Latency:** SLAs must also guarantee maximum network latency of less than 50ms for all services delivered between the CSP's in-country data center and the end-user within Nigeria.
- **4.3.3 Justifiable Variations to SLA Metrics:** The standards defined above are the mandatory default for all mission-critical and citizen-facing government services irrespective of data classification level. However, these network latency and support requirements can be adjusted on a case-by-case basis if a compelling justification is provided in the solution's design. This flexibility is intended for non-critical, internal, or back-office applications where high availability and low latency are demonstrably not essential for the service's primary function. FPIs must formally acknowledge that any decision to procure services with relaxed SLAs will directly impact user experience and may conflict with the government’s commitment to service delivery excellence, as outlined in frameworks like SERVICOM. Therefore, any justification for lower SLA targets must include an impact assessment on citizen satisfaction and overall service quality.

DRAFT

4.4 FPI-Focused Service Offerings from Pre-approved Cloud Service Providers

- **4.4.1 Market Driven Approach:** To simplify procurement for FPIs, this policy encourages a market-driven approach to service offerings while maintaining rigorous oversight. The Digital Marketplace, managed by The Sovereign Cloud Governance Committee (SovGov), will serve as the authoritative directory of certified Cloud Service Providers (CSPs) and Service Integrators (SIs) eligible to provide services to the government.
- **4.4.2 FPI-Ready Service Bundles and the Digital Marketplace:** Instead of NITDA pre-approving specific service bundles, certified Cloud Service Providers (CSPs) and Service Integrators (SIs) are encouraged to create and prominently display "FPI-Ready" service bundles on their own websites and product pages. These bundles should be pre-configured to meet the tiered security, availability, and compliance requirements outlined in this policy.
- **4.4.3 Audit and Delisting of FPI-Ready Service Bundles:** The Digital Marketplace will provide direct links to these FPI-focused offerings on the certified providers' sites. While providers are responsible for creating these bundles, they must ensure that all components and services within a marketed "FPI-Ready" bundle are fully compliant with the standards herein. NITDA reserves the right to audit these offerings and can delist any bundle that fails to meet the required standards.

5.0 Security and Resilience Operations

5.1 Cybersecurity Standards and Controls

- The security of cloud services shall utilize a **Zero Trust Architecture (ZTA)** approach. This principle assumes that no user or device is trusted by default, requiring continuous verification for every access request.
- Encryption for data at rest and in transit must utilize **AES-256 bit encryption or higher**.
- Annual, independent **third-party penetration testing** is mandatory for all CSP and SI infrastructure hosting government data. **Continuous automated vulnerability scanning** must be operational for all internet-facing systems.
- A **Web Application Firewall (WAF)** must be deployed and properly configured to protect all public-facing government web applications and APIs.

5.2 Cloud Governance and Access Management Protocols

- **5.2.1 Foundational Access Controls:** Access must be governed by Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to ensure only authorized personnel can access sensitive government data. Multi-Factor Authentication (MFA) must, at a minimum, utilize Time-based One-Time Password (TOTP) applications. For access to environments hosting Level 3 or 4 data, the use of FIDO2-compliant hardware security keys is mandatory.

- **5.2.2 Network and Location-Based Access Controls:** Access to cloud services

DRAFT

hosting government data classified as Level 2 (Moderate Sensitivity) or higher shall, by default, be restricted to pre-approved Nigerian IP address ranges. Exceptions for legitimate international access (e.g., for diplomatic missions, traveling officials, or approved international partners) must be formally justified, time-bound, and approved through a documented risk assessment process managed by the respective FPI.

- **5.2.3 Privileged Access Management:** All privileged administrative access to the cloud environment must be managed through a Privileged Access Management (PAM) solution. This system must enforce ephemeral access (just-in-time), session recording, and a detailed, immutable audit log of all privileged actions.

5.3 Incident Reporting Procedures

- **5.3.1 Immediate Reporting Obligation:** In accordance with the Shared Responsibility Model, the Federal Public Institution (FPI) holds ultimate accountability for its data. However, the operational duty to report rests with the service providers. Therefore, any personal data breach or significant security incident impacting government data or cloud infrastructure must be reported upon discovery. This obligation falls upon the contracted Service Integrator (SI) and the underlying Cloud Service Provider (CSP).

- **5.3.2 Reporting Timeline and Recipients:** Upon a verified incident, the responsible SI or CSP shall provide immediate notification to:
    - The affected FPI.
    - The Nigeria Data Protection Commission (NDPC), as the statutory authority for data protection.
    - The National Information Technology Development Agency (NITDA), as the lead coordinating body for this policy.

  This notification must be made without undue delay and, in any case, **not later than 72 hours** of becoming aware of a verified incident, as mandated by the Nigeria Data Protection Act (NDP Act) 2023. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the FPI must ensure the affected data subjects are notified immediately.

- **5.3.3 Minimum Content of Breach Notification:** The initial notification report submitted to the NDPC and NITDA must, at a minimum, contain the following information as stipulated in the NDP Act General Application and Implementation Directive (GAID):
    - A description of the circumstances and nature of the breach, including the categories and approximate number of data subjects and personal data records concerned.
    - The date or time period during which the breach occurred.

DRAFT

- An assessment of the likely risk of harm to individuals.
- A description of the measures taken or proposed to be taken to address the breach and mitigate its adverse effects.
- The name and contact information of the designated Data Protection Officer (DPO) or other relevant contact person who can provide further information.

- **5.3.4 Incident Logging and Cooperation:** CSPs and SIs must maintain comprehensive logs and detailed reports of all security incidents, not limited to verified incidents. These records must document the timeline of events, the findings of internal investigations, and all remedial actions taken. These incident logs and reports are critical for forensic analysis and must be made available to national law enforcement and security agencies upon lawful request. CSPs and SIs are required to provide full cooperation to support investigations, national security efforts, and the overall strategic goal of enhancing Nigeria's cybersecurity resilience.

- 5.3.5 Definitions: For the purpose of this section, 'Discovery' is the initial identification of a potential security event. A 'Verified Incident' is an event confirmed, after triage, to be a security breach. The mandatory reporting timeline commences upon the confirmation of a 'Verified Incident'.

5.4 Backup and Disaster Recovery Requirements

- 5.4.1 Vendor Transparency in Disaster Recovery and Backup: Data centers hosting government information must implement comprehensive, tested, and documented disaster recovery (DR) plans to ensure business continuity and the resilience of public services. These plans must include geographically distributed backups and automated failover mechanisms to secondary sites. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are mandatory components of all Service Level Agreements (SLAs). SIs are required to be aware of these
- 5.4.2 System Integrator (SI) Due Diligence: The Service Integrator, in its capacity as the primary provisioning entity for the FPI, is required to conduct thorough due diligence on the DR capabilities disclosed by the CSP. The SI must ensure that the chosen CSP's services align with the specific RTO and RPO requirements mandated in the FPI's Service Level Agreement (SLA). The SI's knowledge and management of these capabilities are critical components of its contractual obligation to the FPI.
- 5.4.3 Audit and Certification Requirement: As a mandatory component of NITDA's certification and annual recertification process, both CSPs and SIs must provide evidence of successful DR testing for the infrastructure hosting government data. This evidence may include recent third-party audit reports (e.g., SOC 2 reports covering

DRAFT

availability) or documented results from a simulated live failover and recovery exercise. Failure to provide satisfactory proof of DR testing may result in the suspension or revocation of certification.

- 5.4.4 **Policy on Cross-Border Transfers for Backup and Disaster Recovery:** To uphold Nigeria's data sovereignty, this policy establishes a **"Nigeria-First"** principle for disaster recovery infrastructure. While fully acknowledging the convenience of utilizing existing infrastructure outside the country to aid in fulfilling redundancy and resilience of cloud services, the objective of this policy is to build capacity within the country for all such services to be provided locally in the near term.
    1. **Primary and Secondary Sites within Nigeria:** For all data classification levels, both the primary production site and the secondary (failover) disaster recovery site **must be located within Nigeria's territorial boundaries**. This ensures that the first lines of data hosting and recovery reside locally, supporting the national digital economy and limiting foreign jurisdiction.
    2. **Prohibition for High-Sensitivity Data:** Under no circumstances shall data classified as LEVEL 4 (Classified) or LEVEL 3 (High Sensitivity) be backed up or transferred outside of Nigeria. All copies, including archival and backup data, must remain within the country.
    3. **Conditional Waivers for Tertiary Backups:** An exception for a *tertiary* (out-of-country) backup is permissible only for data classified as LEVEL 2 (Moderate Sensitivity) and LEVEL 1 (Limited Sensitivity), and only when all of the following stringent conditions are met:
        - **Demonstrable Need:** The FPI must provide a formal justification to NITDA demonstrating that in-country DR sites are insufficient to meet specific, heightened resilience or business continuity requirements that cannot otherwise be fulfilled.
        - **Compliance with the NDP Act 2023:** Any cross-border transfer must be executed in strict accordance with the Nigeria Data Protection Act (NDP Act) 2023. This requires the destination country to either have an **adequacy decision** from the Nigeria Data Protection Commission (NDPC) or for the transfer to be governed by an **approved protective instrument**, such as Standard Contractual Clauses (SCCs).
        - **Mandatory Encryption:** All data transferred and stored in a tertiary backup site outside Nigeria must be encrypted both in-transit and at-rest using security standards specified in the National Cloud Technical Document. The FPI or its SI must ensure that it retains full control over the encryption keys, which must be generated and managed from within Nigeria.
        - **Sovereign Governance Approval:** Before any such arrangement is made, the FPI must obtain explicit, prior written approval from the Sovereign Cloud Governance Committee (SovGov).

DRAFT

4. **Impact on Service Level Agreements (SLAs):** The restrictions on cross-border data transfers detailed in this section may impact the standard Service Level Agreements (SLAs), particularly the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) offered by global Cloud Service Providers (CSPs).
    - Therefore, the Sovereign Cloud Governance Committee (SovGov) is required to conduct a thorough assessment of these impacts during the transition phase of this policy's implementation. This assessment shall be performed in consultation with Federal Public Institutions (FPIs) and accredited CSPs to identify potential conflicts between the policy's data residency requirements and the providers' global disaster recovery architectures.
    - Following the assessment, SovGov shall develop and issue guidance for FPIs on negotiating SLAs that align with this policy while still meeting their operational resilience requirements. This may include frameworks for risk acceptance or templates for customized SLA clauses.

6.0 Technical Guidelines for Migration and Deployment

6.1 Pre-migration Assessment and Planning

- FPIs must conduct a cloud readiness assessment, identify sources of value (efficiency, agility), and create a roadmap for migration. This phase must include a detailed Discovery and Dependency Mapping exercise to catalog all applications, databases, network configurations, and their interdependencies. This prevents service disruptions caused by migrating an application without its required components. Applications must be classified to determine the appropriate migration strategy (e.g., rehost, refactor, re-platform, re-architect). This roadmap shall also include a formal **Rollback Plan**, detailing the procedures to revert to the legacy system in case of an unsuccessful migration.

6.2 Pilot Migration and Validation

- Before a full-scale migration, the SI must execute a **Pilot Migration** involving a small, non-critical subset of the services slated for transition. The purpose of this pilot is to test the migration methodology, validate security controls in the target cloud environment, and confirm performance benchmarks. Learnings from this phase must be documented and used to refine the full migration plan, ensuring a more predictable

DRAFT

and successful outcome.

6.3 Secure Migration Methodologies

- Data migration must be secured using end-to-end encryption and secure transfer protocols (SSL/TLS, IPsec). Data integrity must be verified post-migration using hashing or checksums. Secure transfer protocols for data migration must be configured to use the latest secure versions, specifically **TLS 1.2 or higher**. All migration activities must be logged in an **immutable audit trail** to ensure accountability and support forensic analysis if an incident occurs.

6.4 Post-deployment Validation and Optimization

- After migration, FPIs must validate application performance and data integrity against pre-defined success criteria established during the planning phase. Continuous monitoring of SLAs is required to ensure compliance and drive continuous improvement. Furthermore, the SI must implement a Continuous Optimization and Cost Management (FinOps) process. This involves regularly analyzing cloud usage, right-sizing resources (e.g., adjusting virtual machine sizes to match workload demands), and identifying cost-saving opportunities to ensure that the FPI's cloud expenditure is financially efficient.

6.5 Legacy Infrastructure Decommissioning

- **6.5.1 Framework and Responsibility:** The secure and efficient decommissioning of legacy physical infrastructure is a mandatory final phase of any cloud migration project. While the FPI retains ultimate ownership of and accountability for its legacy assets, the contracted Service Integrator (SI) is responsible for planning, executing, and documenting the entire decommissioning process in accordance with this framework.
- **6.5.2 Decommissioning Plan:** As part of the migration roadmap, the SI must submit a formal **Decommissioning Plan** to the FPI for approval. This plan must include, at a minimum:
    - **Asset Inventory:** A comprehensive inventory of all hardware to be decommissioned, including servers, storage arrays, and networking equipment.
    - **Data Destruction:** A detailed procedure for the secure and permanent sanitization of all data from storage media. The process must align with internationally recognized standards such as **NIST SP 800-88 (Guidelines for Media Sanitization)**. The SI must provide a formal **Certificate of Data Destruction** to the FPI for every storage device.
    - **Environmental Disposal:** A plan for the environmentally sound recycling or disposal of all hardware components, conducted through a government-

DRAFT

certified e-waste management partner. The plan must adhere to all national environmental protection regulations.
    - **Asset Value Recovery:** A process for assessing the residual value of decommissioned assets. The SI shall manage the logistics of remarketing, reallocating, or repurposing viable equipment to "realize value" for the FPI.
    - **Chain of Custody:** A documented and auditable chain of custody that tracks each hardware asset from the point of shutdown to its final disposition (destruction, recycling, or resale).
- **6.5.3 Final Verification:** Upon completion of the process, the SI must submit a Final Decommissioning Report to the FPI, which includes all asset tracking logs, Certificates of Data Destruction, and e-waste disposal receipts. This report serves as the official record of a securely completed migration project.

7.0 Data Sovereignty Compliance

7.1 Technical Compliance Framework for FPIs

- FPIs must use the national Data Classification Framework to categorize their data and ensure it is stored in a cloud environment that meets the required security and residency standards.

7.2 Service Integrator and CSP Reporting Requirements

- **7.2.1 Service Integrator and CSP Reporting Requirements** CSPs and SIs must provide government entities with access to audit logs and compliance dashboards. A standardized infrastructure status report must be submitted to NITDA on a **quarterly basis**, using the template provided in Annex A of this document. This report must capture metrics on location, tier certification, security posture, power, and disaster recovery test results.

7.3 Audit and Verification Procedures

- NITDA and certified third parties will perform regular audits to validate contractually agreed controls. These audits will verify compliance with security, data handling, and localization mandates.

DRAFT

8.0 Data Center and Physical Infrastructure Standards

8.1 Minimum Tier Certification

- All primary and secondary data centers hosting government data must be designed, constructed, and operated to a minimum auditable standard.
    - Facilities hosting Level 4 or Level 3 data must be certified as Uptime Institute Tier III or TIA-942 Rated-3 for both design and constructed facility.
    - Facilities hosting Level 2 data must, at a minimum, meet the requirements of Uptime Institute Tier II or TIA-942 Rated-2.

8.2 Power and Cooling Redundancy

- Power infrastructure must provide a minimum of N+1 redundancy for all critical components, including UPS systems, power distribution units, and backup generators.
- The data center's Power Usage Effectiveness (PUE) must be reported to NITDA annually, with a target of 1.6 or lower to ensure energy efficiency.

8.3 Physical Security Controls

- Physical access to data halls must be governed by a multi-layered security model, requiring a minimum of three distinct authentication factors (e.g., key card, PIN code, biometric scan) for entry.
- 24x7x365 on-site security personnel are mandatory. A comprehensive Closed-Circuit Television (CCTV) system must monitor all perimeter, entry, and critical interior zones, with footage retained for a minimum of 90 days.

9.0 Annexes

To aid in the practical implementation of this policy, the following annexes form an integral part of this technical document:

- **Annex A:** Standardized Template for Quarterly Infrastructure Status Reports
- **Annex B:** Sample Service Level Agreement (SLA) Template
- **Annex C:** Government Risk Assessment and Threat Modelling Tool
- **Annex D:** Cloud Provider Accreditation Checklist
- **Annex E:** Standardized Incident Reporting Form

DRAFT

- **Annex F:** Disaster Recovery Test Attestation Form
- **Annex G:** FinOps and Cloud Cost Reporting Template
- **Annex H:** Framework for Evaluating Foreign CSP Strategic Investment

DRAFT

Annex A: Standardized Template for Quarterly Infrastructure Status Reports

- **Purpose**: To establish a uniform and transparent reporting mechanism for CSPs and SIs, enabling NITDA and FPIs to consistently track the compliance, health, and performance of the cloud infrastructure hosting government data.

Quarterly Infrastructure Status Report

- **Reporting Period**: [Q1, Q2, Q3, Q4] [YEAR]
- **Provider (CSP/SI)**: [Provider Name]
- **FPI Client(s) Covered**: [List of FPIs]

Metric	Current Status	Notes / Changes Since Last Quarter
Data Center Location(s)	[e.g., Ikeja, Lagos; Maitama, Abuja]	[e.g., New availability zone added]
Tier Certification	[e.g., Uptime Institute Tier III - Constructed Facility]	[e.g., Recertification completed on DD/MM/YY]
Security Certifications	[e.g., ISO 27001, CSA STAR, SOC 2 Type II]	[e.g., ISO 27017 certification in progress]
Quarterly Uptime %	[e.g., 99.98%]	[Details of any downtime incidents]
Security Incidents	[Number of major/minor incidents]	[Brief, non-sensitive summary of incidents]
Power Usage Effectiveness (PUE)	[e.g., 1.58]	[e.g., Cooling system upgrade improved PUE]

Annex B: Sample Service Level Agreement (SLA) Template

- **Purpose**: To provide a standardized and comprehensive starting point for SLAs between FPIs and their service providers, ensuring all critical performance, security, and compliance metrics are contractually defined and enforceable.

Key Sections of an FPI Service Level Agreement

1. **Service Description**: Details of the cloud services being provided (e.g., Secure IaaS for Level 3 Data).
2. **Performance Metrics**:
    a. **Availability (Uptime)**: Tiered uptime guarantees (99.9%, 99.95%, 99.99%) based on the data classification level being hosted.
    b. **Network Latency**: Commitment to <50ms latency within Nigeria.
    c. **Recovery Time Objective (RTO)**: [e.g., < 1 hour].
    d. **Recovery Point Objective (RPO)**: [e.g., < 4 hours].
3. **Support and Incident Response**: Tiered 24x7 support response and resolution times based on data classification.
4. **Data Governance**: Commitment to Nigerian data residency, security standards, and the NDP Act 2023.
5. **Penalties for Non-Compliance**: Clear financial penalties (e.g., service credits) for failing to meet agreed-upon metrics.
6. **Exit Strategy**: Procedures for secure data repatriation and deletion upon contract termination.

DRAFT

Annex C: Government Risk Assessment and Threat Modelling Tool

- **Purpose**: To provide a simple, standardized framework for FPIs and SIs to identify, assess, and mitigate risks associated with migrating and operating services in the cloud.

Sample Risk Register

Risk ID	Risk Description	Impact (1-5)	Likelihood (1-5)	Risk Score (I x L)	Mitigation Plan	Owner
001	Data breach due to misconfigured access controls	5	3	15	Implement PAM; conduct quarterly access reviews.	SI
002	Service outage due to DR failover failure	5	2	10	Conduct annual live DR failover test.	CSP/SI
003	Non-compliance with data residency for Level 3 data	4	2	8	Configure location-based policies; regular audits.	SI
004	Unauthorized access of cloud services	5	4	20	Train FPI employees on proper security practices. Zero Trust Architecture.	SI/FPI

Annex D: Cloud Provider Accreditation Checklist

- Purpose: To outline the core criteria that will form the basis of the official NITDA certification checklist, ensuring a transparent and comprehensive evaluation process for all providers.

Governance and Oversight

- The certification process for all Cloud Service Providers (CSPs) and Service Integrators (SIs) seeking inclusion in the government's Digital Marketplace shall be managed by NITDA in partnership with the Sovereign Cloud Governance Committee (SovGov). This process ensures that all providers meet the mandatory security, operational, and compliance standards outlined in this policy.

Illustrative Accreditation Criteria

The summary below is illustrative and is intended to highlight the spirit in which the official checklist will be created, focusing on key domains of compliance.

- Corporate Compliance:
  - Valid registration with the Corporate Affairs Commission (CAC).
  - Current Tax Clearance Certificate.
  - Demonstrated adherence to the Guidelines for Nigerian Content Development in ICT.
- Technical Standards:
  - Data Center Tier Certification (e.g., Uptime Institute, TIA-942).
  - Evidence of adherence to or a formal roadmap for achieving relevant ISO certifications
  - Current SOC 2 Type II and/or CSA STAR attestation reports.
- Security Controls:
  - Proof of annual, independent third-party penetration testing.
  - Documentation of a security framework aligned with Zero Trust Architecture principles.
  - Details of implemented Privileged Access Management (PAM) and Multi-Factor Authentication (MFA) solutions.
- Data Sovereignty Compliance:
  - Attestation of the technical capability to host all data classes securely within Nigeria.
  - Documentation of in-country encryption and key management protocols.
- Requirements for Strategic Investment Waiver:
  - Minimum technical and investment requirements to qualify for and maintain strategic investment waiver which grants foreign CSPs indigenous status and

DRAFT

listing in the Digital Marketplace. This could include phased data center construction timelines, minimum Tier certification for local facilities, and local talent development targets.

Provisional Certification Pathway

- To foster the development of local industry and ensure Nigerian providers can compete, a **Provisional Certification** pathway is established. This allows indigenous CSPs making verifiable progress towards meeting all required international standards to be listed on the Digital Marketplace. For the purpose of fair competition, a Provisional Certification will be listed with the same standing as a Full Certification and will not be indicated differently on the Marketplace.
- To qualify for Provisional Certification, an indigenous provider must submit the following to NITDA:
    - A documented and board-approved **roadmap to achieve full certification** within a maximum period of **24 months**.
    - Verifiable evidence of having formally **engaged a certified auditor** to conduct a gap analysis and guide the implementation of required controls.
- Providers holding a Provisional Certification may be restricted, at the discretion of NITDA and SovGov, to hosting government data classified only as **LEVEL 1 (Limited Sensitivity)** and **LEVEL 2 (Moderate Sensitivity)**. This status is subject to a mandatory **annual review** by NITDA to assess progress. Provisional Certification will be revoked if satisfactory progress towards full certification is not demonstrated.

DRAFT

Annex E: Standardized Incident Reporting Form

- **Purpose**: To ensure that data breach notifications submitted to NITDA and the NDPC are consistent, complete, and contain all necessary information for a rapid and effective regulatory response.

Data Breach Notification Form

- Section 1: Incident Overview
  - **Reporting Organization**: [CSP/SI Name]
  - **Affected FPI(s)**: [FPI Name]
  - **Date and Time of Discovery**: [DD/MM/YYYY HH:MM]
  - **Date and Time Range of Breach**: [DD/MM/YYYY to DD/MM/YYYY]
  - **Nature of Breach**: [e.g., Ransomware, Unauthorized Access, Misconfiguration]
- Section 2: Impact Assessment
  - **Data Classes Involved**: [e.g., PII, Financial Records]
  - **Estimated Number of Data Subjects Affected**: [Number]
  - **Assessment of Risk/Harm to Individuals**: [Low/Medium/High, with justification]
- Section 3: Response and Mitigation
  - **Measures Taken to Contain Breach**: [Description of actions]
  - **Plan to Notify Affected Individuals (if required)**: [Yes/No, with timeline]
- Section 4: Contact Information
  - **DPO / Primary Contact**: [Name, Email, Phone]

DRAFT

Annex F: Disaster Recovery Test Attestation Form

- **Purpose**: To provide a formal, standardized document for service providers to certify that successful disaster recovery tests have been completed, fulfilling a key requirement for NITDA accreditation.

Disaster Recovery Test Attestation

This form attests that **[Provider Name]** successfully completed a disaster recovery test for the cloud infrastructure supporting **[FPI Name / "All Government Clients"]**.

- **Date of Test**: [DD/MM/YYYY]
- **Type of Test**: [e.g., Full Failover Simulation, Tabletop Exercise]
- **Outcome**: **[ ] SUCCESSFUL [ ] PARTIAL SUCCESS [ ] UNSUCCESSFUL**
- **Summary of Results**: The test confirmed a successful failover to the secondary site located in [City, Nigeria]. The RTO of [e.g., 45 minutes] and RPO of [e.g., 5 minutes] were met.
- **Attested By (Third-Party Auditor, if applicable)**: [Auditor Name/Firm]
- **Provider Representative**: [Name, Title, Signature]

DRAFT

Annex G: FinOps and Cloud Cost Reporting Template

- **Purpose**: To provide a standardized framework for SIs to report on cloud spending to FPIs, ensuring fiscal transparency and accountability. This template also serves as the required format for mandatory submission to the Sovereign Cloud Governance Committee (SovGov), enabling its whole-of-government cost aggregation and negotiation functions as stipulated in the National Cloud Policy 2025.

Quarterly Cloud Cost and Optimization Report

- **Reporting Period**: [Q1, Q2, Q3, Q4] [YEAR]
- **FPI Name**: [FPI Name]
- **Prepared By**: [SI Name]

Category	Amount (NGN)	Notes / Key Changes
Total Cloud Spend (This Quarter)		
Spend by Service (Top 5)	[e.g., Compute, Storage, Database]	[e.g., Increased compute for new e-service]
Budget vs. Actual Spend	[Budget: NGN, Actual: NGN, Variance: %]	[Explanation for variance]
Cost Savings Achieved		[e.g., NGN saved via reserved instances]
Cost Optimization Recommendations		[e.g., Decommission unused resources, right-size VMs]

Of course. Here is a guide for evaluating the strategic investment of foreign Cloud Service Providers (CSPs), which can be included as an appendix in the National Cloud Technical Document.

First, here are some additional categories of investment and support to consider including in the evaluation, building upon your initial list:

- **Local Research & Development (R&D):** Establishing physical R&D centers in Nigeria or providing direct funding for technology research at Nigerian universities.
- **Startup Ecosystem Development:** Creating venture funds, accelerators, or incubator programs specifically for Nigerian tech startups, beyond just offering cloud credits.
- **Investment in Renewable Energy:** Direct investment in local renewable energy projects (e.g., solar or wind farms) to power data center operations, contributing to both digital and green infrastructure goals.
- **Local Supply Chain Development:** Actively procuring services, materials, and non-critical hardware from local Nigerian businesses for their operations, thereby stimulating the broader economy.
- **Public Sector Digital Literacy:** Funding and executing broad digital literacy and cloud skills programs for government employees and the general public, beyond the specialized training for SIs.

DRAFT

Annex H: Framework for Evaluating Foreign CSP Strategic Investment

- **Purpose:** This framework provides a standardized guide for the Sovereign Cloud Governance Committee (SovGov) to evaluate the degree and strategic value of investments made by foreign Cloud Service Providers (CSPs) in Nigeria. The evaluation will inform decisions regarding procurement priority, the granting of temporary data localization waivers, and eligibility for strategic partnerships under the National Cloud Policy 2025 (NCP2025).
- **Evaluation:** The framework uses a color-coded system to classify the level of investment commitment.
    - **GREEN (Strongest Investment):** Indicates a direct, significant, and long-term capital investment in Nigeria's physical, economic, or human capital infrastructure. These actions directly support the core objectives of data sovereignty and local content development.
    - **BLUE (Case-by-Case Determination):** Represents a valuable contribution but one that requires further assessment of its long-term impact and strategic alignment. These actions are positive but may be less capital-intensive or more commercially focused.
    - **GRAY (Lukewarm Investment):** Describes actions that are minimal, primarily sales-driven, or leverage global programs with no specific commitment to the Nigerian ecosystem.

Category 1: Local Data Center Infrastructure

This evaluates direct investment in physical data center facilities within Nigeria.

Level	Criteria for Evaluation
GREEN	• Direct capital investment in the construction and operation of a **hyperscale availability region** with **multiple availability zones** within Nigeria. • Facility(ies) must be certified as **Uptime Institute Tier III** (or TIA-942 Rated-3) for both design and constructed facility. • Demonstrable use of local construction, engineering, and facilities management firms.

DRAFT

BLUE	• Investment in a **single availability zone** or a dedicated local zone for specific services. • A fully-funded, time-bound commitment (≤ 24 months) with financial guarantees to build a local data center. • A long-term, high-capacity co-location agreement with an indigenous data center provider where the CSP owns and manages all core compute, storage, and network hardware.
GRAY	• Reliance on data centers located in other African countries (e.g., South Africa, Kenya) to serve Nigerian customers. • Presence is limited to an edge location or a network Point-of-Presence (PoP) only. • Vague or non-committal statements about future data center investments.

Category 2: Network Connectivity Infrastructure

This evaluates investment in the core network infrastructure that enhances national and international connectivity.

Level	Criteria for Evaluation
GREEN	• Direct capital investment in **landing new subsea cables** in Nigeria. • Funding and construction of **terrestrial fiber optic backbone** routes that connect multiple states or underserved regions. • Establishing multiple, high-bandwidth peering points at local Internet Exchange Points (IXPs).
BLUE	• Significant investment in dedicated, redundant last-mile fiber connectivity to major government, enterprise, or tech hubs. • Co-investment partnerships with local telecommunication companies to

	expand fiber infrastructure.
GRAY	• Sole reliance on leasing capacity from existing network providers. • Peering at a single IXP with no significant dedicated bandwidth investment.

Category 3: Application & Service Localization

This evaluates the extent to which a CSP's platform and services are tailored for the Nigerian market.

Level	Criteria for Evaluation
GREEN	• Full localization of the cloud platform, including user interfaces, technical documentation, and customer support in **major Nigerian languages**. • Full integration with Nigeria's financial system, including **billing in Nigerian Naira (NGN)** and direct integration with local payment gateways. • Development of **Nigeria-specific cloud services** or features that address local industry needs (e.g., in fintech, agriculture, healthcare).
BLUE	• Platform available in English only but with full NGN billing and local payment support. • Basic localization of marketing materials and sales support.
GRAY	• Platform and support are English-only. • Billing is exclusively in a foreign currency (e.g., USD). • Services are generic global offerings with no adaptation to the Nigerian context.

Category 4: Training & Capacity Building for SIs and Partners

This evaluates investment in developing the local technical and commercial partner ecosystem.

Level	Criteria for Evaluation
GREEN	• Establishment of a **physical training and certification center** in Nigeria. • A comprehensive, locally-run program to train and certify Nigerian SIs and partners on technical, security, and governance tracks, offered at **no cost or heavily subsidized**. • Provision of dedicated, in-country partner development and technical support teams.
BLUE	• Partner enablement programs that are **primarily marketing-driven**, focused on co-selling and lead generation. • Provision of online training vouchers and subsidies for remote certification exams.
GRAY	• Reliance on global online training resources with no localized content or support. • Partner programs that require high fees or have significant barriers to entry for Nigerian companies.

Category 5: Local IT Industry & Startup Ecosystem Support

This evaluates direct contributions to fostering innovation and growth in Nigeria's broader tech industry.

Level	Criteria for Evaluation

GREEN	• Establishment of a **local Venture Capital (VC) fund** or a formal partnership with a Nigerian VC to invest in tech startups. • Creation and funding of a local **startup accelerator or incubator program** in Nigeria. • Establishment of a **local R&D center** focused on cloud technologies or related fields.
BLUE	• Offering significant, long-term cloud credits to startups registered in recognized Nigerian tech hubs. • Sponsoring major local tech conferences and innovation challenges. • Ad-hoc partnerships with universities or tech hubs without sustained funding.
GRAY	• Global startup programs that Nigerian companies can apply to, but with no specific local track or resources. • Minimal engagement with the local tech community beyond sales and marketing efforts.

Other Strategic Considerations

In addition to the criteria above, SovGov will take the following factors into account to form a holistic view of a CSP's strategic commitment to Nigeria:

- **Global Regulatory Compliance History:** The CSP's track record in other jurisdictions regarding compliance with data protection laws (e.g., GDPR), including any history of significant penalties or sanctions for non-compliance.
- **Public Sector & Citizen Digital Skills Development:** The degree of investment in broad-based digital literacy programs for government employees and the general public, including partnerships with educational institutions to develop a national digital skills curriculum.
- **Local Supply Chain Development:** The CSP's commitment to procuring services and materials from local Nigerian businesses for its operations (e.g., facilities management, marketing, legal services), thereby contributing to the broader local economy.
- **Adherence to Data Ethics:** The CSP's demonstrable commitment to ethical data handling, particularly in the deployment of AI and automated systems, in alignment with the principles outlined in the NDP Act General Application and Implementation Directive (GAID).
- **Commitment to Open Standards:** The CSP's approach to interoperability and the use of open standards (e.g., Open Virtualization Format) to prevent vendor lock-in, which is a key objective of the NCP2025.

- **Investment in Renewable Energy:** The extent to which the CSP invests directly in local renewable energy sources (e.g., solar farms) or enters into long-term Power Purchase Agreements (PPAs) with Nigerian green energy providers to power its infrastructure, as opposed to relying on diesel generators.
- **Transparent Protocols for Lawful Data Access:** The existence of clear, legally compliant, and transparent processes for responding to lawful requests for data access from Nigerian government and security agencies, in accordance with the NDPA and Mutual Legal Assistance Treaties (MLATs).

DRAFT