FEDERAL REPUBLIC
OF NIGERIA

National Digital Cloud Policy

Acronyms and Abbreviations 4
PART I: ECONOMIC IMPERATIVES AND MARKET DEVELOPMENT 6
1. Strategic Context and Market Opportunity **7**
1.1 The Global Cloud Transformation 7
1.2 Nigeria's Competitive Position 7
1.3 The Regional Export Opportunity 9
1.4 The Case for Policy Intervention 10
1.5 Purpose and Approach of this Policy 10
1.6 Scope and Application 11
1.7 Baseline Assumptions 11
2. Policy Objectives **12**
2.1 Attract Investment in Cloud and Data Infrastructure 12
2.2 Develop Nigeria as a Regional Digital Services Exporter 12
2.3 Expand and Diversify Domestic Capacity 12
2.4 Build a Competitive, Multi-Provider Market 12
2.5 Develop Indigenous Capability and Participation 12
2.6 Modernise Government Service Delivery 12
2.7 Achieve Value for Money in Public Expenditure 12
2.8 Enable Interoperability and Open Standards 12
2.9 Secure Government and Regulated Data Proportionately 13
3. Investment Attraction and Incentives **13**
3.1 Purpose and Principles 13
3.2 Fiscal Incentives 13
3.3 Anchor Demand as an Investment Incentive 14
3.4 Regulatory Facilitation and Investment Certainty 14
3.5 Capital Mobility and Foreign Exchange Treatment 15
3.6 Energy Access as an Investment Incentive 15
3.7 Partnership, Technology Transfer and Local Participation 15
3.8 Eligibility and Qualification 16
3.9 Monitoring Incentive Effectiveness 16
4. Regional Trade and Digital Services Export **16**
4.1 The Regional Market 16
4.2 Regional Hosting Hub Development 16
4.3 Cross-Border Data Flows and Trade Facilitation 17
4.4 Regulatory Interoperability and Standards Alignment 17
4.5 Export Promotion and Market Development 17
4.6 Openness and Non-Discrimination 19
5. Enabling Infrastructure: Energy, Connectivity and Distribution **19**
5.1 Energy and Power Infrastructure 19
5.2 Geographic Distribution and National Resilience 20
5.3 Connectivity and Interconnection 21
6. Capacity Development and Skills **21**
6.1 Priority Areas 22
6.2 Institutional Arrangements 22
PART II: GOVERNMENT CLOUD ADOPTION **23**
7. Cloud Adoption in Government **24**
7.1 Cloud First Adoption 24
7.2 Exemptions 24
7.3 Progressive Migration of Existing Systems 24
7.4 Rationalising On-Premise Infrastructure 24
7.5 Alignment of ICT Procurement 25

8. Whole of Government Aggregation Framework **25**
8.1 Aggregation Model 25
8.2 Exceptions to Default GBB Hosting 25
8.3 Non-Exclusivity 25
8.4 Hybrid Deployment 26
9. Procurement and Marketplace Framework **26**
9.1 National Digital Marketplace 26
9.2 Aggregated Procurement 26
9.3 Marketplace Structure and Governance 26
9.4 Contractual Safeguards 27
9.5 Coordinated Procurement 27
10. Funding and Commercial Framework **27**
10.1 Dedicated Cloud Budget Lines 27
10.2 Ringfenced Anchor Capacity Funding 27
10.3 Negotiated Rates 28
10.4 Service Level and Institutional Arrangements 28
10.5 Support for State Governments and Subnational Entities 28
PART III: SOVEREIGNTY FOR GOVERNMENT AND REGULATED DATA **29**
11. Sovereignty Framework for Government and Regulated Data **30**
11.1 Purpose and Justification 30
11.2 Sovereign Data Defined 30
11.3 Classification Framework 31
11.4 Residency and Control Requirements 32
11.5 Cross Border Processing 32
11.6 Designation of Regulated Data as Sovereign Data 32
11.7 Presidential Approval 33
11.8 Security and Access Control 33
11.9 Portability and Interoperability Safeguards 33
11.10 Enforcement and Compliance 33
12. Institutional Roles and Governance for Sovereign Data **34**
12.1 Allocation of Functions 34
12.2 Galaxy Backbone Limited (GBB) 34
12.3 GBB Institutional Development 35
12.4 National Information Technology Development Agency (NITDA) 35
12.5 Office of the National Security Adviser (ONSA) 35
12.6 Bureau of Public Procurement (BPP) 36
12.7 Sovereign Government Cloud Governance Committee 36
PART IV: IMPLEMENTATION AND REVIEW **38**
13. Implementation Roadmap **39**
13.1 Phase 1: Activation and Baseline (0 to 6 Months) 39
13.2 Phase 2: Deployment and Market Activation (6 to 12 Months) 39
13.3 Phase 3: Scale and Export Development (12 to 24 Months) 39
13.4 Implementation Governance 39
14. Monitoring, Evaluation and Review **40**
14.1 Performance Monitoring and Reporting 40
14.2 Policy Review 40
14.3 Market, Security and Risk Assessment 40
14.4 Key Performance Indicators 40
14.5 Policy Position 42

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Policy.

ACRONYM	MEANING
3MTT	Three Million Technical Talent Programme
AfCFTA	African Continental Free Trade Area
AI	Artificial Intelligence
API	Application Programming Interface
BPP	Bureau of Public Procurement
CBN	Central Bank of Nigeria
DBI	Digital Bridge Institute
ECOWAS	Economic Community of West African States
FEC	Federal Executive Council
FMCIDE	Federal Ministry of Communications, Innovation and Digital Economy
GBB	Galaxy Backbone Limited
ICT	Information and Communications Technology
IXP	Internet Exchange Point
KPI	Key Performance Indicator
MDA	Ministry, Department or Agency of the Federal Government (plural MDAs)
NCG	National Cloud Guideline 2026
NCTG	National Cloud Technical Guideline 2026
NDIAF	National Digital Infrastructure Assurance Framework
NDPA	Nigeria Data Protection Act 2023
NDPC	Nigeria Data Protection Commission
NEPC	Nigerian Export Promotion Council
NERC	Nigerian Electricity Regulatory Commission
NIMC	National Identity Management Commission
NITDA	National Information Technology Development Agency
ONSA	Office of the National Security Adviser
PUE	Power Usage Effectiveness, a measure of data centre energy efficiency
SBG	Strategic Business Group
SGCGC	Sovereign Government Cloud Governance Committee, established under Part 12.7
SLA	Service Level Agreement
SOC	Security Operations Centre
SOE	State Owned Enterprise
SSA	Sub-Saharan Africa

PREAMBLE

The National Digital Cloud Policy establishes a national framework for the growth, governance and internationalisation of Nigeria's cloud and data infrastructure . It seeks to attract investment, develop Nigeria as a regional hosting and digital services export hub, modernise government service delivery through disciplined cloud adoption and aggregated purchasing, and apply proportionate sovereignty requirements to the defined category of government and regulated data.

The Policy retains an open and multi-provider market approach. Generally the policy promotes and preserves cross border data flows, while carefully incorporated sovereignty controls are risk-based and limited to defined categories of data. Government adoption is supported through Cloud First, whole-of-government aggregation, coordinated procurement, dedicated budgeting and an anchor-demand framework. Implementation is supported by institutional roles for NITDA, GBB, BPP and the Sovereign Government Cloud Governance Committee, together with a phased implementation roadmap and measurable KPIs.

PART I:

Economic Imperatives And Market Development

1. Strategic Context and Market Opportunity

1.1 The Global Cloud Transformation

The rapid global expansion of cloud computing has fundamentally transformed how economies organise production, how institutions deliver services, and how nations manage their most critical digital assets. Cloud infrastructure now underpins financial services, commerce, healthcare, education, logistics, manufacturing, and public administration, and it constitutes the foundation upon which artificial intelligence, advanced data analytics, and successive generations of digital services are being built. Organisations that once acquired and operated their own computing infrastructure increasingly consume computing as a service, converting capital expenditure into operating expenditure and gaining access to capabilities that few institutions could develop independently.

The scale of this transformation is considerable. The global public cloud services market is projected to reach approximately USD 1.28 trillion by 2028, reflecting sustained double-digit annual growth driven by accelerating adoption across governments and industries.[1] The infrastructure supporting this market, comprising data centres, subsea and terrestrial fibre networks, energy systems, and the specialised workforce required to design and operate them, has emerged as a category of national economic infrastructure comparable in strategic significance to ports, power generation, and transport networks.

For countries situated as Nigeria is, this transformation presents both a significant economic opportunity and an important strategic consideration. Digital infrastructure of this nature must be located somewhere, and the jurisdictions that host it attract investment, generate employment, broaden their revenue base, and develop exportable capability. Conversely, where a country hosts little of the infrastructure upon which its digital economy depends, the value created within that economy tends to accrue elsewhere, and the systems underpinning public services and critical national sectors may remain beyond the effective reach of domestic law and regulatory oversight.

This Policy is framed to address both dimensions, prioritising investment, market development, and regional competitiveness, while, in Part III, establishing the measured arrangements necessary to secure national control over government and regulated data.

1.2 Nigeria's Competitive Position

For Nigeria, the opportunity is both significant and strategic, and the case for investment rests on assets the country already possesses rather than on aspiration alone.

As Africa's most populous country and one of its largest digital markets, Nigeria recorded 142,161,409 active internet subscriptions as of January 2025, providing the scale of domestic demand necessary to sustain digital infrastructure at a commercially viable level, a threshold that most markets within the subregion are unable to reach independently.

Nigeria's international connectivity further reinforces this position. The country is currently served by eight international submarine cable systems, comprising SAT-3/WASC, MainOne, Glo-1, ACE, WACS, Equiano, 2Africa, and NCSCS,[2] providing substantial international bandwidth and establishing Nigeria as a natural landing, transit, and interconnection point for the West African subregion.

[1] Gartner, "Forecast: Public Cloud Services, Worldwide, 2022-2028, 2Q24 Update," Gartner, accessed July 23, 2026, https://www.gartner.com/en/documents/5541595.

[2] Submarine Networks, "Nigeria," Stations: Africa, https://www.submarinenetworks.com/en/stations/africa/nigeria.

Complementing this connectivity advantage, the Federal Government has launched the 90,000 km National Fibre Optic Backbone Project, one of Africa's largest broadband infrastructure initiatives, aimed at expanding nationwide broadband access, improving digital inclusion, and strengthening the country's digital economy.[3] By extending high-capacity terrestrial connectivity beyond the coastal corridor, the Project is expected to improve the economics of hosting outside Lagos and render viable a range of locations that have not previously supported commercial digital infrastructure.

Project BRIDGE: Building Resilient Digital Infrastructure for Growth

Project BRIDGE is an Initiative of the Federal Government of Nigeria, established to deploy at least 90,000 km of fibre-optic cable as Nigeria's core connectivity infrastructure and national backbone, under a public-private partnership funding model, thereby completing the 120,000 km rollout target identified in the National Broadband Plan 2020 to 2025. Unveiled by the Minister of Communications, Innovation and Digital Economy at a Lagos stakeholder forum, it will raise the national fibre footprint from approximately 35,000 km to 125,000 km, representing the largest fibre backbone investment in any developing country.

Design

Seven regional backbone rings interconnect Nigeria's six geopolitical zones and Lagos, forming a resilient national framework that ensures redundancy, minimises latency, and supports seamless data flow across the country. The network is wholesale and open-access, structured to serve both large and small internet service providers through core, metropolitan, and middle-mile layers, enabling competition and shared infrastructure. Thirty-seven metropolitan networks connect all 774 local government areas.

Structure and financing

The estimated total cost is USD 2 billion, funded through a combination of development finance institution debt and private-sector equity, with the government holding a minority stake of not less than 25 per cent, capped at 49 per cent. The investment will be managed independently as a limited liability SPV company with its own board. Over USD 600 million had been secured from the World Bank, EBRD, and the EU by the first quarter of 2026, and the African Development Bank subsequently approved USD 200 million for the project, which is aligned with Vision 2050, the National Development Plan, and the Renewed Hope Development Plan 2026 to 2030.

[3] World Bank, "Nigeria Accelerates Digital Inclusion with $500 Million World Bank Backed Project," World Bank, https://www.worldbank.org/en/news/press-release/2025/06/26/nigeria-accelerates-digital-inclusion-with-500-million-world-bank-backed-projectopen-access, structured to serve both large and small internet service providers through core, metropolitan, and middle-mileThirty-sevenThe estimated total cost is USD 2 billion, funded through a combination of development finance institution debt and private-sector equity, with the government holding a minority stake of not less than 25 per cent, the EU by the first quarter of 2026, and the African Development Bank subsequently approved USD 200 million for the project, which is , established to deploy at least 90,000 km of fibre-optic cable as Nigeria's core connectivity infrastructure and national backbone, under a public-private partnership funding model, thereby .

Recognising that digital capability depends as much upon human capital as upon physical infrastructure, the Federal Government launched the Three Million Technical Talent (3MTT) Programme to develop a globally competitive workforce equipped with the skills required to support cloud computing, artificial intelligence, cybersecurity, software engineering, and other emerging technologies.[4] The availability of such capability is among the principal considerations informing investment decisions in this sector.

These initiatives are pursued within the broader digital economy agenda of the Federal Ministry of Communications, Innovation and Digital Economy, which provides the policy direction and institutional coordination necessary for their coherent implementation.[5]

A growing number of domestic and international data centres and cloud operators have established or expanded operations in Nigeria, and private-sector demand for hosting capacity is projected to exceed 283 MW within 15 years, compared with public-sector demand of approximately 10 MW over the same period. Growth in installed capacity will therefore be driven principally by commercial demand, with the government participating as a substantial and coordinating customer rather than as the dominant source of demand.

Taken together, these assets position Nigeria to become a leading regional hub for digital and cloud services. What has been required is a coherent policy framework capable of translating these advantages into committed investment, installed capacity, and sustained export earnings.

1.3 The Regional Export Opportunity

Beyond the domestic market, Nigeria is well positioned to serve the wider West African and Sub-Saharan African region. Most markets in the subregion are too small individually to support hyperscale infrastructure. Demand across these markets is real and growing, yet it remains fragmented across numerous jurisdictions and is presently served, in large measure, from data centres located in Europe. This arrangement imposes recurring costs upon the region, including latency that impairs application performance, transit costs that raise the price of digital services, and foreign exchange outflows that might otherwise be retained within the continent.

Considered in aggregate, however, regional demand is substantial and lies well within the reach of Nigerian infrastructure. The country combines cable landings, backbone capacity, market scale, a deepening talent base, and an increasingly credible regulatory environment. With deliberate policy support, Nigerian data centres and cloud service providers are capable of hosting workloads for enterprise, financial, and public-sector customers across ECOWAS and the wider Sub-Saharan African market, thereby establishing digital services as an export sector, as other economies have established financial and professional services.

The Federal Government recognises that this opportunity is time-sensitive. Regional hosting arrangements, once established, tend to endure, as migration costs and accumulated integration dependencies discourage customers from relocating workloads. Those jurisdictions that establish themselves as regional hubs within the current investment cycle may be expected to retain that position for a considerable period. Nigeria's advantages, while substantial, are neither exclusive nor permanent, and other markets within the region are actively pursuing the same investment.

Accordingly, this Policy treats the development of regional service export capability as a primary objective rather than as an incidental benefit of domestic market growth, and Part 4 sets out the measures through which this objective will be pursued.

[4] 3MTT, "Shaping the Future of Nigeria's Digital Workforce," 3 Million Technical Talent Programme, https://3mtt.nitda.gov.nginforming investment decisions in Nigeria, and private-sector demand for hosting capacity is projected to exceed 283 MW within 15 years, compared with public-sector.
[5] Federal Ministry of Communications, Innovation and Digital Economy, "Driving Economic Growth Through Digital Technology and Innovation," https://fmcide.gov.ng hub for digital and cloud services.

1.4 The Case for Policy Intervention

Notwithstanding these advantages, Nigeria has not yet attracted installed capacity at the scale the market would support. The constraints are identifiable, and each can be addressed through deliberate policy action.

- **Energy reliability**

  Grid supply, rather than demand, is the binding constraint on data centre growth generally. Facilities must provide their own generation, materially increasing capital costs and lengthening development timelines.
- **Fiscal treatment**

  Data centre equipment and the power and cooling systems that support it incur duties and charges that raise Nigerian project costs relative to competing locations.
- **Regulatory friction**

  Approvals required for infrastructure development are distributed across multiple institutions without coordination, introducing delays and uncertainty into investment decisions.
- **Foreign exchange exposure**

  Providers price currency risk into their offers, and government purchasers have historically borne that risk on an institution-by-institution basis rather than managing it collectively.
- **Fragmented public demand**

  Government cloud spending has been dispersed across institutions, producing neither the commercial leverage nor the demand signal that a coordinated buyer of its scale should command.

- **Absence of coordination**

  No single framework has governed how government cloud demand is planned, procured, classified, hosted, or monitored, with the result that the Cloud First principle adopted in 2019 was implemented unevenly.[6]

Each of these is a coordination or policy failure rather than a market failure that policy cannot address. The subsequent Part of this Policy address these issues directly and provide a pathway for developing data centres and cloud capacity in Nigeria.

1.5 Purpose and Approach of this Policy

This Policy establishes the national framework for the growth, governance, and internationalisation of Nigeria's cloud and data infrastructure sector. Its purposes are, in order of emphasis:

- to attract and retain investment in cloud and data centre infrastructure in Nigeria;
- to develop Nigeria as a regional hosting and digital services export hub for West Africa and Sub-Saharan Africa;
- to modernise government service delivery through disciplined cloud adoption and aggregated purchasing; and
- to establish clear, proportionate sovereignty requirements for the narrow category of government and regulated data where national control is genuinely necessary.

The approach in this policy is deliberately open and inclined to Nigeria's commitment to trade in digital services. A cardinal objective is to ensure Nigeria's market is open to domestic and international providers on transparent and predictable terms. However, sovereignty requirements under Part III apply to a defined and limited class of data and are not a general restriction on where commercial data may be hosted or processed. The overwhelming majority of economic activity in Nigeria's cloud market falls outside those requirements and is governed by basic commercial and regulatory law, including the Nigeria Data Protection Act 2023.[7]

[6] Nigeria Cloud Computing Policy 2019, which introduced the Cloud First principle for Federal Public Institutions.
[7] Nigeria Data Protection Act 2023, Laws of the Federation of Nigeria.on-premises

This Policy does not pursue technological isolation, nor does it treat foreign participation as a risk to be managed. It treats global capability, deployed in Nigeria and connected to Nigerian firms and Nigerian talent, as the fastest available route to a competitive domestic industry. A hybrid approach, in which infrastructure located in Nigeria operates alongside international capacity within a common governance framework, is adopted throughout in preference to localisation mandates.

1.6 Scope and Application

Parts I and IV of this Policy apply generally and establish the framework for investment, trade, market development, and implementation.

Part II applies to Federal Ministries, Departments and Agencies and to entities exercising public functions on their behalf. State Governments, the Federal Capital Territory, and Local Governments may participate voluntarily under Part 10.5.

Part III applies to sovereign data as defined in Part 11.2, comprising data generated by the Federal Government and data generated under Federal regulation, licence, or directive that has been designated under Part 11.6. It does not apply to commercial data outside that definition.

1.7 Baseline Assumptions

All targets and performance indicators under this Policy are measured against the following baseline assumptions, which reflect the current state rather than an idealised starting point:

- **Partial and fragmented cloud utilisation**

  Cloud adoption across MDAs is partial, uneven, and uncoordinated, mixing legacy on-premises systems with ad hoc commercial subscriptions. Standard partial utilisation of cloud resources, rather than mature enterprise adoption, is therefore the planning baseline for migration targets, capacity forecasting, and cost modelling.
- **Absence of an organised framework**

  No single framework has governed how government cloud demand is planned in, procured, classified, hosted, or monitored in Nigeria. MDAs have procured independently, resulting in duplicated expenditure, inconsistent security postures, and a lack of consolidated visibility into government workloads. This absence, rather than the availability of technology, has been the principal constraint on adoption since 2019.
- **Lack of deliberate skills requirements and pathways**

  Public sector cloud, cybersecurity, and data competencies have developed incidentally, without mandatory standards, certification requirements, or structured career pathways governing the personnel who design, procure, and operate government systems. This Policy treats workforce capability as a designed input under Part 6.

The Key Performance Indicators in Part 14.4 are calibrated against this starting position, and baseline values will be established through the audit required under Part 13.1.

2. Policy Objectives

The objectives of this Policy, in order of priority, are as follows.

2.1 Attract Investment in Cloud and Data Infrastructure

Establish Nigeria as the most attractive destination in West Africa for investment in data centres, cloud infrastructure, subsea and terrestrial connectivity, and artificial intelligence compute capacity. This will be pursued through competitive fiscal treatment, regulatory predictability, coordinated facilitation, and reliable anchor demand, applied without discrimination between qualifying investors.

2.2 Develop Nigeria as a Regional Digital Services Exporter

Position Nigeria as the hosting, processing, and interconnection hub for West Africa and Sub-Saharan Africa, so that regional workloads are served from Nigerian infrastructure, regional traffic is exchanged within Nigeria, and digital services become a recognised export earning sector contributing to foreign exchange receipts.

2.3 Expand and Diversify Domestic Capacity

Grow installed hosting capacity substantially and distribute it across the federation, reducing the concentration risk arising from the present clustering of capacity in Lagos and extending the economic benefits of digital infrastructure investment to regions currently underserved.

2.4 Build a Competitive, Multi-Provider Market

Maintain an open and contestable market in which domestic and international providers compete on transparent terms, and in which customers, including government, retain genuine choice, data portability, and the practical ability to switch providers without prohibitive cost.

2.5 Develop Indigenous Capability and Participation

Deepen the participation of Nigerian firms and professionals across the cloud value chain through structured partnerships, technology transfer, and skills development, so that domestic capability grows alongside international investment rather than competing with it, and so that the pool of Nigerian firms able to compete regionally expands over time.

2.6 Modernise Government Service Delivery

Improve the cost, security, resilience, and speed of public digital services by adopting cloud as the default deployment model for government workloads, consolidating shared services, and eliminating the duplication inherent in institution-by-institution infrastructure provision.

2.7 Achieve Value for Money in Public Expenditure

Consolidate fragmented government cloud spending into aggregated arrangements that deliver materially lower unit costs, predictable multi-year budgeting, and stronger contractual protections than individual institutions can secure alone.

2.8 Enable Interoperability and Open Standards

Ensure that government and regulated systems interoperate through open standards and documented interfaces, supporting integrated service delivery, competitive procurement, avoidance of vendor lock-in, and interconnection with regional systems.

2.9 Secure Government and Regulated Data Proportionately

Apply clear, risk-based sovereignty requirements to the defined class of government and regulated data where national control is necessary, in a manner that is proportionate to identified risk, transparent in application, narrowly targeted, and subject to periodic review, as set out in Part III.

Implementation of these objectives shall be measured through the Key Performance Indicators in Part 14.4. Baseline values shall be established and validated within six months of adoption, and targets may be refined where necessary to reflect the findings of the baseline assessment, subject to the review arrangements under Part 14."

3. Investment Attraction and Incentives

3.1 Purpose and Principles

This Part is the principal instrument of the Policy. The Federal Government will deploy a coordinated package of fiscal, regulatory, commercial, and facilitation incentives to attract investment in cloud and data infrastructure and to make Nigeria the most competitive hosting location in the subregion.

Incentives are directed at a specific objective, being the installation of physical capacity in Nigeria and the development of the capability to operate it. They are structured to address the identified constraints in Part 1.4 rather than to subsidise activity that would occur regardless. All incentives under this Part shall be administered transparently and subject to applicable laws, statutory approvals, fiscal sustainability considerations and published eligibility criteria.
The following principles govern their design and administration:

- **Non-discrimination:** Eligibility turns on the nature and scale of the investment made in Nigeria, not on the nationality, ownership, or domicile of the investor.
- **Transparency:** Qualification criteria are published in advance, applied objectively, and subject to review, enabling investors to assess eligibility before committing capital.
- **Proportionality:** The value of incentives received is matched by the scale of investment and the capability commitments undertaken.
- **Predictability:** Incentive terms for a qualifying investment remain stable over the investment horizon, in accordance with applicable law.
- **Accountability:** Incentive effectiveness is monitored, reported, and periodically reviewed against the outcomes it is intended to produce.

3.2 Fiscal Incentives

Fiscal treatment is the most direct lever available and addresses the cost differential identified in Part 1.4. Qualifying investments in cloud and data centre infrastructure will be eligible for the following support, applied in accordance with applicable fiscal and investment law:

- Import duty exemptions, waivers, or concessions on data centre equipment, including servers, storage systems, networking equipment, racks, cabling, and associated components.
- Extension of the same duty treatment to power generation, energy storage, cooling, and environmental control equipment required for qualifying deployments, recognising that these represent a substantial share of total project cost in the Nigerian operating environment and that their exclusion would materially reduce the value of the incentive.
- Access to preferred status and equivalent tax incentives for qualifying strategic digital infrastructure projects, where the applicable statutory criteria are met.

- Capital allowance treatment appropriate to the long asset life and high upfront capital intensity of data centre investment.
- The value-added tax treatment of exported cloud and data services is consistent with Nigeria's treatment of other exported services, so the tax system does not penalise exports of regional services.
- Clarity of tax treatment for cross-border service delivery, so that providers serving foreign customers from Nigerian infrastructure can determine their obligations with certainty.

The Federal Ministry of Finance, the National Revenue Service, and the Nigeria Customs Service will, in consultation with NITDA, issue implementation guidance specifying the categories of qualifying equipment, eligibility thresholds, application procedures, and verification requirements. Guidance will be published and maintained in published form.

3.3 Anchor Demand as an Investment Incentive

The Federal Government will use its own aggregated purchasing as a commercial incentive for infrastructure investment. Government expenditure on cloud services will be incurred in any event; aggregating it converts that expenditure into a catalytic instrument.

- Government cloud demand will be aggregated through the national aggregation framework established under Part 8, with GBB serving as the aggregation and resale platform, creating a demand signal of sufficient scale to support project finance.
- Providers that establish qualifying infrastructure in Nigeria will be eligible to compete for aggregated offtake opportunities on published, objective criteria.
- Long-term anchor offtake agreements, backed by the Anchor Capacity Fund established under Part 10.2, will provide the contractual certainty that infrastructure lenders and investment committees require before committing capital to long-lived assets.
- Offtake commitments will be structured with tenors appropriate to infrastructure financing, and insulated from annual budget volatility through the ringfencing arrangements in Part 10.2.
- Qualification criteria will be published in advance, applied transparently, and reviewed periodically.

Anchor demand addresses the fundamental difficulty in infrastructure investment: capacity must be built before demand can be served, and investors require assurance that demand will materialise.

3.4 Regulatory Facilitation and Investment Certainty

Regulatory friction is a material deterrent to infrastructure investment, and delay is itself a cost. The Federal Government will accordingly:

- Establish a single coordinated facilitation point for qualifying cloud and data centre investments, assisting in obtaining business licences, regulatory permits, construction approvals, environmental clearances, and operational authorisations.
- Designate qualifying projects as strategic national digital infrastructure, attracting expedited regulatory processing and priority administrative handling across relevant institutions.
- Publish, and maintain in published form, the licensing, compliance, and operational requirements applicable to cloud and data infrastructure investment, so that requirements are ascertainable in advance rather than discovered in the course of development.
- Coordinate across investment promotion, industrial regulation, planning, revenue, and energy institutions to eliminate duplicative approval requirements and reduce administrative delay.
- Establish and publish service standards for the determination of applications, with performance against those standards reported under Part 14.
- Provide, where appropriate, stabilisation assurances in respect of the fiscal and regulatory terms applicable to qualifying long-term investments, in accordance with applicable law.

3.5 Capital Mobility and Foreign Exchange Treatment

Investors require confidence that returns can be realised and repatriated. Currency risk has been identified as a principal concern of international providers assessing the Nigerian market. Accordingly:

- Lawful repatriation of capital, profits, and dividends is permitted in accordance with applicable investment and foreign exchange regulations.
- Qualifying investments will be issued with the certificates and registrations necessary to secure repatriation rights, with coordinated administrative support to avoid procedural delay.
- Government aggregated arrangements will, where feasible, incorporate Naira-denominated or currency risk-managed pricing structures. GBB will pool and manage foreign exchange exposure on behalf of participating institutions, reducing the risk that individual providers would otherwise price it into their offers and that individual MDAs are poorly placed to manage it.
- Earnings from cloud and data services exported to customers outside Nigeria will be treated as export earnings for applicable foreign exchange and export incentive frameworks.
- Relevant institutions will clarify the treatment of cross-border payments for cloud services, enabling both providers and customers to plan with certainty.

3.6 Energy Access as an Investment Incentive

Reliable power is the binding constraint on data centre growth in Nigeria, and energy provision is treated in this Policy as an investment incentive rather than merely a technical requirement. A facility that must fund its own generation faces a materially different investment case from one that can rely on grid supply, and policy that ignores this will not attract capacity at scale.
Part 5.1 sets out the measures in full, comprising dedicated and captive generation support, power purchase and wheeling frameworks, fiscal treatment of energy equipment under Part 3.2, and coordinated planning between the digital and energy sectors.

3.7 Partnership, Technology Transfer and Local Participation

Investment incentives are intended to build durable domestic capability alongside international capital. Providers benefiting from incentives under this Part will accordingly implement structured capability development programmes, comprising:

- Measurable knowledge transfer programmes, including technical training and professional certification;
- Skills transfer initiatives aligned with national workforce development frameworks, including the 3MTT Programme;
- Participation of Nigerian professionals in infrastructure deployment, operations, and management roles, with progression pathways into senior technical positions;
- Collaboration with recognised Nigerian training and research institutions;
- Progressive localisation of operational capability over the life of the investment, measured against agreed milestones.

These commitments are structured as partnership obligations rather than market access barriers. They apply to investors receiving public incentives; they are proportional to the value of the incentive received, and they are designed to expand the pool of Nigerian firms and professionals capable of competing in the regional market. They do not restrict participation by investors who do not seek incentives.

Implementation of this Part will give effect to the participation accorded to Nigerian providers under President Bola Ahmed Tinubu's Renewed Hope Nigeria First Policy, the Guidelines for Nigerian Content Development in ICT 2019 and Presidential Executive Orders 003 and 005,[9] applied in a manner consistent with Nigeria's international trade commitments and with the openness principles in Part 1.5. The Strategic Investment Waiver mechanism, administered by NITDA on the recommendation of the Sovereign Government Cloud Governance Committee, is available where an investor's demonstrated commitment to Nigerian infrastructure, employment, and capability development warrants equivalent treatment.

[8] 3MTT, "Shaping the Future of Nigeria's Digital Workforce," 3 Million Technical Talent Programme, https://3mtt.nitda.gov.ng.
[9] Guidelines for Nigerian Content Development in Information and Communications Technology 2019, issued by the National Information Technology Development Agency; Presidential Executive Order 003 of 2017 on Support for Local Content in Public Procurement; Presidential Executive Order 005 of 2018 on Planning and Execution of Projects, Promotion of Nigerian Content in Contracts and Science, Engineering and Technology.

3.8 Eligibility and Qualification

Incentives under this Part are available to providers that demonstrate:

- Deployment, or committed planned deployment, of qualifying infrastructure in Nigeria;
- Registration in the applicable class under the Digital Infrastructure Assurance Registration scheme;
- Participation in the National Digital Marketplace framework, where seeking government business;
- Alignment with national interoperability requirements;
- Compliance with applicable data protection, cybersecurity, and consumer protection obligations;
- Capability development commitments proportionate to the incentive sought, under Part 3.7;
- Clear documentary requirements, decision timelines, compliance monitoring arrangements and a review mechanism.

NITDA, in collaboration with BPP, GBB, and the Federal Ministry of Finance, will issue and publish detailed qualification criteria, application processes, and compliance mechanisms governing access to incentives. Criteria will be objective, published in advance, and applied without discrimination between qualifying investors. Determinations will state reasons, and refusals will be subject to review. No incentive shall be granted or continued where the qualifying investment or associated commitments are materially unfulfilled.

3.9 Monitoring Incentive Effectiveness

- The value of incentives granted, and the investment, capacity, and employment outcomes attributable to them, will be monitored and reported annually.
- Incentive effectiveness will be assessed as part of the review under Part 14.2, and instruments that are not producing the intended outcomes will be revised or withdrawn.
- Compliance with capability development commitments under Part 3.7 will be verified, and continued eligibility will depend on demonstrated performance.

4. Regional Trade and Digital Services Export

4.1 The Regional Market

Nigeria's ambition is to become the location from which West African and Sub-Saharan African cloud and data workloads are served. The commercial logic is straightforward. Serving a customer in Accra, Abidjan, or Dakar from a facility in Lagos or Abuja delivers materially lower latency than serving them from Frankfurt or London, at lower transit cost, and with settlement that can occur within the continent.

The constraint has not been demand but supply, and the response required is not protection but capacity. This Part sets out the trade and market access measures through which regional service export will be pursued.

4.2 Regional Hosting Hub Development

The Federal Government will actively develop Nigeria's capability to host and process workloads originating outside Nigeria.

- **Regional demand aggregation:** The government will support Nigerian providers in marketing capacity to customers across ECOWAS and the wider Sub-Saharan African market, including through trade missions, market intelligence, and coordinated positioning of Nigeria's connectivity and capacity advantages.
- **Interconnection and transit:** The development of Internet Exchange Points and regional peering arrangements will be prioritised to enable regional traffic to be exchanged and workloads to be served within Nigeria rather than routed through Europe.
- **Landing station and backbone access:** Terms of access to submarine cable landing stations and national backbone capacity will support competitive transit and hosting offers to regional customers, and will be monitored for their effect on the competitiveness of Nigerian providers.

- **Latency and cost advantage:** Government will support the commercial case that hosting West African workloads in Nigeria delivers materially lower latency and cost than serving them from European facilities, including through independent measurement and publication of performance data.
- **Regional public sector demand:** Nigeria will explore arrangements under which regional institutions and neighbouring governments may access hosting capacity in Nigeria under appropriate legal and commercial terms.

4.3 Cross Border Data Flows and Trade Facilitation

Nigeria's ability to export digital services depends on data moving lawfully across borders. A country cannot become a regional hosting hub while maintaining restrictions that prevent foreign data from entering it or foreign customers from relying on it. The Federal Government will accordingly:

- Maintain a predictable and transparent framework for cross-border data transfer, including the publication and periodic updating of a list of jurisdictions recognised as providing adequate protection under the Nigeria Data Protection Act 2023.[10] The absence of such a published list has been a source of uncertainty for both providers and customers.
- Ensure that data protection and localisation requirements are proportionate, risk-based, and confined to the categories where they are necessary, so they do not become unnecessary barriers to trade in services.
- Pursue mutual recognition and adequacy arrangements with priority trading partners, so that Nigerian providers can serve foreign customers without duplicative compliance burdens and foreign customers can rely on Nigerian infrastructure with confidence.
- Ensure that measures adopted under this Policy are consistent with Nigeria's commitments under the African Continental Free Trade Area, including its Protocol on Digital Trade, and with other applicable international trade obligations.
- Publish determination timeframes for cross-border authorisation applications and report performance against them under Part 14.

4.4 Regulatory Interoperability and Standards Alignment

Regulatory divergence raises the cost of regional service delivery and reduces the credibility of Nigerian providers to foreign customers. The Federal Government will therefore:

- Align Nigerian cloud, data protection, and infrastructure assurance standards with recognised international standards, so that compliance in Nigeria is recognised elsewhere.
- Engage in ECOWAS and African Union processes on digital trade, data governance, and cloud regulation, to promote convergence around standards that Nigerian providers already meet.
- Support the mutual recognition of registration and assurance outcomes with regional counterparts, reducing duplicative certification for providers operating across multiple markets.
- Ensure that the Digital Infrastructure Assurance Registration scheme is designed to be intelligible and credible to international customers, investors, and insurers.

4.5 Export Promotion and Market Development

- Cloud and data services delivered from Nigeria to customers abroad will be recognised as service exports and supported through applicable export promotion instruments.
- The Nigerian Export Promotion Council, in collaboration with NITDA and the Federal Ministry of Industry, Trade and Investment, will incorporate digital and cloud services into national export development programming, including market intelligence, trade facilitation, and buyer engagement.
- The government will support Nigerian providers in obtaining the international certifications and assurances required by foreign enterprises and public-sector customers.
- Performance in regional service export will be monitored and reported under Part 14, including capacity contracted to non-Nigerian customers and associated export earnings.

[11] Agreement Establishing the African Continental Free Trade Area, and the Protocol on Digital Trade adopted there under.

Technology Export and Digital Trade Desk

The Federal Government has established a Technology Export and Digital Trade Desk within the Federal Ministry of Communications, Innovation and Digital Economy, in collaboration with the Federal Ministry of Industry, Trade and Investment. Trade constitutes the fifth pillar of the Ministry's Strategic Blueprint. The Desk provides the institutional framework through which Nigerian technology exports are promoted, and digital trade relations across the continent are strengthened.

Rationale

Nigeria's technology sector is among the fastest growing in Africa. Yet the country's position on the Economic Complexity Index, at 127th, reflects limited diversity and sophistication in its export portfolio compared with more technologically advanced economies. The Desk was conceived to address that gap, drawing on the experience of China, South Korea, Estonia, Israel, India, and Singapore, each of which has employed government-backed trade promotion machinery to globalise its technology ecosystem and thereby raise total factor productivity.

Objectives

The Desk is directed at four ends: promoting Nigerian technology exports by identifying products and services with export potential and assisting companies in navigating international trade regulations and compliance standards; facilitating intra African digital trade under the African Continental Free Trade Area, including the elimination of tariffs on digital services; ensuring Nigeria's representation in global digital trade agreements so that national interests are advanced in the international digital economy; and improving Nigeria's Economic Complexity Index by enhancing the diversity and sophistication of exported technologies.

Functions

The Desk provides market intelligence, including country specific reports on trade requirements, regulatory barriers, and technology trends; facilitates export logistics and compliance, covering export procedures, intellectual property protection, and international standards; organises trade missions, technology showcases, and international exhibitions for business matchmaking; delivers capacity building and export readiness programmes, including advisory support on product localisation, pricing, and global marketing; and builds partnerships with other ministries, private sector organisations, and international trade bodies. Additionally, the Desk shall coordinate, as appropriate, with relevant trade, investment and regulatory institutions to reduce administrative barriers to the export of cloud, hosting, data processing and related digital services.

4.6 Openness and Non-Discrimination

Nigeria's regional ambition depends on Nigeria itself being an open market. A country that seeks to host its neighbours' data cannot maintain unjustified restrictions on hosting its own data, and cannot expect regional partners to extend treatment it does not itself offer.

- Accordingly, and subject only to the sovereignty requirements applying to the defined class of data in Part III, this Policy:
- does not restrict where commercial data generated in Nigeria may be hosted or processed;
- does not discriminate between providers based on nationality, ownership, or domicile;
- does not require the use of Nigerian infrastructure for commercial workloads; and
- does not condition market access on local establishment, except where a provider seeks incentives or government business under the terms set out in this Policy.

Requirements imposed under Part III are targeted, justified by identified national interest, and subject to the review and approval disciplines set out in that Part.

5. Enabling Infrastructure: Energy, Connectivity and Distribution

Infrastructure investment follows infrastructure readiness. This Part addresses the physicalpreconditions for a competitive hosting industry.

5.1 Energy and Power Infrastructure

Reliable power is a prerequisite for cloud infrastructure. Grid reliability, rather than demand, is the binding constraint on data centre growth in Nigeria, and facilities are presently required to provision dedicated generation as a condition of operation. The Federal Government will therefore treat the provision of energy for digital infrastructure as an integral component of this Policy.

- **Dedicated power:** Registered facilities will be supported to establish dedicated, embedded, or captive generation, including gas, solar, and hybrid systems, with priority processing of associated permits and licences.
- **Power purchase frameworks:** Relevant authorities will facilitate power purchase agreements, eligible customer arrangements, and wheeling frameworks allowing qualified operators to contract supply directly from generation companies.
- **Transition and Clean energy:** Incentives under Part 3 will apply preferentially to facilities integrating transition energy sources, renewable generation, storage, or verified emissions reductions, thereby aligning capacity growth with national energy transition commitments.
- Efficiency standards: NITDA will issue minimum energy-efficiency standards for registered facilities, including Power Usage Effectiveness benchmarks, which will be tightened progressively as the market matures.
- **Fiscal support:** Duty exemptions under Part 3.2 extend to power generation, storage, and cooling equipment for qualifying deployments.
- **Coordination:** NITDA and GBB will align energy planning with projected hosting demand, in coordination with the Federal Ministry of Power, NERC, the Rural Electrification Agency, and state electricity regulators, taking into account projected public-sector demand of approximately 10 MW and private-sector demand exceeding 283 MW.

National Data Park, Egbin: Co-locating Compute with Generation

The Federal Government has identified Egbin, Lagos State, as the host location for Nigeria's first National Data Park and Compute Infrastructure, to be developed in collaboration with the operators of the Egbin Power Plant. Egbin is West Africa's largest privately operated power station, with an installed capacity of 1,320 MW, and already supplies over 16 per cent of the national grid. Its scale, together with access to deep-sea internet cable infrastructure and over 500 hectares of available land, positions the site as a premier location for digital infrastructure.

In announcing the designation, the Minister of Communications, Innovation and Digital Economy identified the plant's reliable power supply, expansive land, access to water, and capable management as the essential conditions for a digital economy hub. The initiative aligns with the National Artificial Intelligence Strategy launched in 2024 and aims to enable Nigeria's digital transformation and facilitate sustainable value extraction from the digital economy.

The Park is envisaged to comprise Tier III and Tier IV data centre facilities, dedicated power infrastructure with renewable energy integration, high-capacity fibre connectivity and internet exchange capability, and associated research, development, and training facilities. Development is proposed under a public-private partnership structure, with fiscal and regulatory incentives to be extended through designation as a technology trade-free zone.

Energy resilience and Power Usage Effectiveness benchmarks will constitute qualification criteria for registration under the Digital Infrastructure Assurance Registration scheme, applied through the Operational Compliance class, with siting criteria assessed at Approval in Principle.

5.2 Geographic Distribution and National Resilience

In Nigeria today, Data centre capacity is currently concentrated in Lagos. This creates concentration risk. This leaves other regions underserved, and confines the economic benefits of digital infrastructure investment to a single corridor. The Federal Government will pursue deliberate geographic distribution.

- Regional clusters: The government will promote strategically located clusters beyond Lagos, including Abuja and viable locations across the country, guided by connectivity, power availability, security, and demand.
- Backbone alignment: Siting and incentives will align with the national fibre backbone expansion, including the planned 90,000 km project,[12] to make hosting viable outside coastal corridors.
- Investment weighting: Incentives under Part 3 may be weighted to favour deployment in underserved regions, reflecting the national interest in distributed capacity.

[12] World Bank, "Nigeria Accelerates Digital Inclusion with $500 Million World Bank Backed Project," World Bank, https://www.worldbank.org/en/news/press-release/2025/06/26/nigeria-accelerates-digital-inclusion-with-500-million-world-bank-backed-project.

- Siting criteria: NITDA will issue siting guidance covering power, connectivity, physical security, environmental risk, and proximity to demand.
- Geographic redundancy: For the workload classes identified in Part 11, recovery capability must be maintained at a facility geographically separated from the primary site, in a different geopolitical zone or at such distance as to ensure continuity in the event of localised disruption.

5.3 Connectivity and Interconnection

- The government will support the expansion of Internet Exchange Point capacity and domestic peering, so that Nigerian traffic is exchanged in Nigeria and regional traffic can be exchanged there as well.
- Access arrangements for submarine cable landing stations and national backbone capacity will support competitive hosting and transit offers, consistent with Nigeria's position as a landing point for eight international cable systems.[13]
- Backbone expansion will prioritise underserved regions, extending the range of viable hosting locations beyond existing clusters.
- The government will monitor international bandwidth pricing and availability as determinants of the competitiveness of Nigerian hosting.

6. Capacity Development and Skills

Sustained sectoral growth depends on the availability of skilled personnel, both in the industry and in the institutions that regulate it and buy from it. Skill constraints directly affect investment decisions, since investors assess whether a location can staff and operate the facilities they build.

3MTT: Building the Technical Talent Backbone

The Three Million Technical Talent (3MTT) programme is a critical component of the Renewed Hope agenda, aimed at building Nigeria's technical talent backbone to power the digital economy and to position the country as a net exporter of technical talent. Launched in 2023, it seeks to train three million Nigerians in high-demand technical skills, contributing to the objective of creating two million digital jobs and reaching learners among youths, graduates, and underserved communities without requiring prior technical knowledge.

Structure and reach

The first phase, executed in collaboration with NITDA, commenced in December 2023 with 30,000 fellows selected across all 36 states and the Federal Capital Territory, combining self-paced online courses with physical applied learning sessions delivered in partnership with over 120 organisations. The second phase is designed to train a further 270,000 technical talents across three successive cohorts. Three cohorts have been completed, training 135,000 fellows through 200 active learning centres nationwide, using structured applied learning rather than short-term bootcamp models. Over 1.8 million applications have been received.

Skills coverage

Training addresses software development, data science, cybersecurity, cloud computing, and artificial intelligence, which closely align with the priority areas identified in Part 6.1 of this Policy.

[13] Submarine Networks, "Nigeria," Stations: Africa, https://www.submshort-termarinenetworks.com/en/stationalign withs/africa/scale-upclosely align withnigeriathe .

Partnership and financing

The programme transitioned from pilot into full implementation as 3MTT 2.0 with the launch of the 3MTT Partner Network in March 2026, supported by an additional €11 million from the European Union and the Government of Denmark. Pioneer corporate partners include IHS Towers, MTN, Airtel, AWS, Google, Microsoft, Huawei, Moniepoint, the EU, and UNDP. The scale-up phase incorporates the Nigeria Talent Cities Initiative, which aims to establish a network of outsourcing campuses and unlock 500,000 jobs by 2027.

6.1 Priority Areas

The following areas will be prioritised for local capacity development:

- Cloud architecture, engineering, migration, and operations;
- Cybersecurity, including security operations, threat monitoring, and incident response;
- Data engineering, data governance, and artificial intelligence;
- Cloud financial management, procurement, and contract administration;
- Data centre design, construction, commissioning, and facilities operation;
- Regulatory and assurance capability within institutions exercising oversight under this Policy.

6.2 Institutional Arrangements

- NITDA, in collaboration with the Digital Bridge Institute and recognised training institutions, will establish a national cloud competency framework defining required competencies, certification pathways, and progression routes for public sector personnel.
- Skills development commitments undertaken by providers receiving incentives under Part 3.7 will be coordinated with the 3MTT Programme[14] and national workforce development frameworks, so that private commitments reinforce public programmes rather than duplicating them.
- MDAs will identify cloud, security, and data roles within their establishments and ensure that personnel occupying them meet applicable competency standards.
- State government personnel participating under Part 10.5 will be eligible for training and certification under this Part.
- Capacity development will extend to non-technical stakeholders and decision makers within MDAs, including procurement, finance, legal, and audit functions, whose decisions materially affect cloud adoption outcomes.
- GBB will develop internal capability in multicloud architecture, platform engineering, cybersecurity, data infrastructure, and commercial operations, in accordance with Part 12.2.

[14] 3MTT, "Shaping the Future of Nigeria's Digital Workforce," 3 Million Technical Talent Programme, https://3mtt.nitda.gov.ng.

PART II:

Government Cloud Adoption

7. Cloud Adoption in Government

The government is potentially the largest single buyer in Nigeria's cloud market and the institution whose service delivery stands to gain most from modernisation. Coordinated government adoption serves two purposes under this Policy: it improves public services, and it generates the demand signal on which Part 3.3 depends.

7.1 Cloud First Adoption

All MDAs will adopt cloud as the default deployment model for new digital systems, services, and workloads. This confirms and operationalises the Cloud First principle introduced in 2019,[15] which was adopted in principle but implemented unevenly in the absence of the governance, funding, and aggregation arrangements established by this Policy. Going forward:

- New systems will be designed for cloud deployment unless an approved exemption applies.
- Business cases for new digital systems must demonstrate that cloud options have been assessed before alternative approaches are considered.
- NITDA will apply this requirement through the ICT project clearance process.
- Cloud adoption decisions will consider total cost of ownership over the system lifecycle rather than initial acquisition cost alone.

7.2 Exemptions

Exemptions from Part 7.1 may be granted where cloud deployment is not appropriate on national security, technical, or operational grounds. Exemption criteria shall be published and applied consistently. Each approved exemption shall identify the workload concerned, the justification, duration, review date and any compensating controls required.

- Applications for exemption will be assessed by NITDA against published criteria and determined within published timeframes.
- Exemptions will be time-bound, subject to periodic review, and recorded in a register maintained by NITDA.
- Exemptions on national security grounds will be determined in consultation with ONSA.
- The grant of an exemption does not relieve an MDA of obligations under Part III where sovereign data is involved.

7.3 Progressive Migration of Existing Systems

- MDAs will assess existing systems and prepare migration plans identifying workloads suitable for cloud deployment, sequenced by business value, risk, technical readiness, and cost.
- Migration will be phased to avoid service disruption and allow institutional capability to develop alongside it.
- The baseline audit under Part 13.1 will establish the inventory of existing systems from which migration planning proceeds.
- GBB will provide migration support, tooling, and advisory services to MDAs under Part 12.2.

7.4 Rationalising On-Premise Infrastructure

- Investment in new on-premises server and storage infrastructure will require justification against cloud alternatives through the ICT project clearance process.
- Existing on-premises infrastructure will be maintained through its economic life and rationalised at natural refresh points rather than prematurely retired, avoiding the destruction of value in serviceable assets.
- This provision is intended to avoid duplicative capital expenditure, not to prohibit on-premises deployment where it is demonstrably appropriate.

[15] Nigeria Cloud Computing Policy 2019, which introduced the Cloud First principle for Federal Public Institutions.

7.5 Alignment of ICT Procurement

- ICT procurement by MDAs will align with this Policy and with the aggregated arrangements established under Part 9.
- BPP and NITDA will ensure that procurement processes and project clearance processes operate consistently and do not impose contradictory requirements on MDAs.

8. Whole of Government Aggregation Framework

Fragmented purchasing has led to duplicate expenditure, inconsistent security postures, and weak commercial terms. Aggregation addresses all three, and simultaneously creates the demand signal on which investment attraction depends.

8.1 Aggregation Model

Aggregation will operate through two complementary layers.

i. Capacity Aggregation as the commercial layer. GBB will aggregate government demand for cloud capacity from multiple registered providers, including international and domestic operators, and resell it to MDAs under framework agreements. This secures volume-based pricing unavailable to individual institutions, maintains a multi-provider environment, and enables utilisation to be optimised across government as a whole rather than institution by institution.

ii. Shared Workload Aggregation is the operational layer.
GBB will design, deploy, and operate shared platforms and services used across government, comprising:
   - Core government platforms, including shared applications and common business systems used by multiple institutions;
   - Horizontal shared services, including access management, governmental payments processing, messaging, notification, and analytics services;
   - Foundational infrastructure services, including backup, disaster recovery, security operations and threat monitoring, and government standard cloud landing zones.

Aggregating at both layers avoids the outcome in which institutions procure and operate systems separately, differing only in ownership. The approach aligns governments' aspirations and reinforces sovereignty, national development and efficiency in government utilisation of cloud capabilities,

8.2 Exceptions to Default GBB Hosting

- MDAs may host external GBB arrangements where technical, operational, or commercial grounds justify doing so, subject to NITDA clearance.
- Applications will be assessed against published criteria and determined within defined timeframes, with reasons given.
- Approved exceptions remain subject to the applicable requirements of this Policy, including Part III where sovereign data is involved and the contractual safeguards required under Part 9.4.

8.3 Non-Exclusivity

GBB's role is to aggregate demand and operate shared services, not to foreclose the market or to substitute a public monopoly for a private one. The aggregation and shared-services role shall not confer on GBB the regulatory, supervisory or market-exclusion authority over competing providers. Framework arrangements shall preserve genuine provider choice, portability and exit rights. Therefore, aggregation is not exclusive and will be implemented through the following approaches:

- Framework arrangements will accommodate multiple providers, and MDAs will retain genuine choice within them.
- Architectures that create exclusive dependency on a single vendor for critical workloads will be avoided.
- Portability and exit rights will be preserved contractually, and providers will be required to support documented migration paths.
- GBB's operational role confers no supervisory or regulatory authority over competing providers, in accordance with Part 12.1.

8.4 Hybrid Deployment

Aggregated arrangements will be implemented on a hybrid basis, combining infrastructure in Nigeria with international capacity into a single coordinated architecture. Sovereignty is exercised through classification, residency requirements, encryption key custody, and contractual safeguards rather than through physical localisation of every workload.

- Workloads subject to residency requirements under Part III will be placed accordingly.
- Other government workloads may use hybrid or international environments where cost, scale, or capability advantages exist.
- GBB will offer hybrid patterns as standard packages, including burst-to-cloud, primary-with-secondary-recovery, and multicloud configurations.
- Placement will be reviewed periodically, enabling progressive migration of workloads to Nigerian infrastructure as domestic capacity, pricing, and provider maturity develop.

9. Procurement and Marketplace Framework

The Federal Government will operate a coordinated procurement and marketplace framework to ensure that acquisition of cloud services across MDAs is efficient, transparent, competitive, and aligned with the objectives of this Policy.

9.1 National Digital Marketplace

- Cloud services for government will be procured through the National Digital Marketplace, administered by NITDA for registration and listing, governed by BPP for procurement compliance, and operated by GBB for aggregation, framework agreements, and chargeback.
- Listing requires a valid Certificate of Registration in the applicable class under the Digital Infrastructure Assurance Registration scheme, and lapses automatically where that registration expires, is suspended, or is revoked.
- The listing is open to domestic and international providers that meet the published criteria and are consistent with Part 4.6.
- The marketplace will maintain the authoritative record of registered providers and available services.

9.2 Aggregated Procurement

- MDA procurement will be effected through aggregated framework agreements, with direct procurement outside those arrangements requiring exception clearance under Part 8.2.
- Aggregated procurement will align with the investment and market incentive mechanisms established in Part 3 and 10.
- Registered Service Integrators may be engaged as delivery and integration partners within framework agreements, providing implementation and managed services beneath the aggregation layer.

9.3 Marketplace Structure and Governance

- The marketplace will publish standardised service catalogues, transparent unit pricing, and comparable service-level terms, enabling MDAs to compare offers consistently.
- Onboarding requirements, catalogue structure, product standardisation, and governance rules will be issued jointly by NITDA, BPP, and GBB.
- Consumer protection measures for MDAs will include disclosure of technical limitations, portability implications, and transition costs.
- Marketplace operations will be monitored for competitive effects, and rules will be adjusted where they are found to favour incumbents or to restrict entry.

9.4 Contractual Safeguards

Framework agreements will incorporate enforceable provisions covering:

- Availability, performance, and service credits;
- Security obligations, incident notification, and audit rights;
- Data portability, export in non-proprietary formats, and documented exit assistance;
- Price transparency and review mechanisms;
- Applicable law, dispute resolution, and remedies;
- Business continuity and disaster recovery obligations.

9.5 Coordinated Procurement

- NITDA and BPP will jointly monitor cloud procurement to identify duplicative or uncoordinated acquisitions, and unapproved procurements will not receive ICT project clearance or procurement approval.
- Annual budget submissions involving cloud or hosting expenditure will be reconciled against the aggregation framework.
- Accounting officers are responsible for ensuring that cloud procurement within their institutions conforms to this Policy.

10. Funding and Commercial Framework

The implementation gap following the 2019 National Cloud Policy was driven substantially by the absence of dedicated funding and predictable commercial arrangements. A policy that mandates adoption without funding it will not be implemented, and this Part addresses that directly.

10.1 Dedicated Cloud Budget Lines

- All MDAs will establish a dedicated recurrent budget line for cloud services, recognising that cloud services convert capital expenditure into recurring operational expenditure and that budget structures designed for capital acquisition do not accommodate this.
- The Budget Office of the Federation, in collaboration with NITDA, will issue circular guidance to standardise the classification, estimation, and approval of cloud expenditure across government.
- MDAs may enter into multiyear service commitments within approved appropriation frameworks, unlocking committed-use pricing and providing providers with predictable demand.

10.2 Ringfenced Anchor Capacity Funding

- A ringfenced Anchor Capacity Fund will back the aggregated purchase commitments of the Federal Government, enabling GBB to enter long-term anchor offtake agreements with registered providers.
- The Fund will underwrite baseline capacity, including shared workloads, disaster recovery, and priority migrations, insulating anchor commitments from budget volatility and virement.
- Sources may include dedicated appropriations, digital economy funds, and co-investment from development finance and infrastructure investment institutions, structured in accordance with applicable fiscal laws.
- Anchor capacity secured under the Fund establishes the government as a creditworthy anchor customer, de-risking private investment in infrastructure and accelerating capacity expansion in accordance with Part 3.3.

10.3 Negotiated Rates

- GBB will negotiate rates with registered providers based on the aggregate scale of government use, securing pricing that is materially below the rates available to any single MDA.
- Arrangements will include committed-use discounts, transparent unit pricing, price review mechanisms, and, where feasible, Naira-denominated or currency-risk-managed pricing.
- Negotiated pricing delivers lower unit costs, budget predictability, elimination of duplicative individual procurements, stronger contractual safeguards than any single agency could secure, and a demand signal strong enough to catalyse long-term investment.

10.4 Service Level and Institutional Arrangements

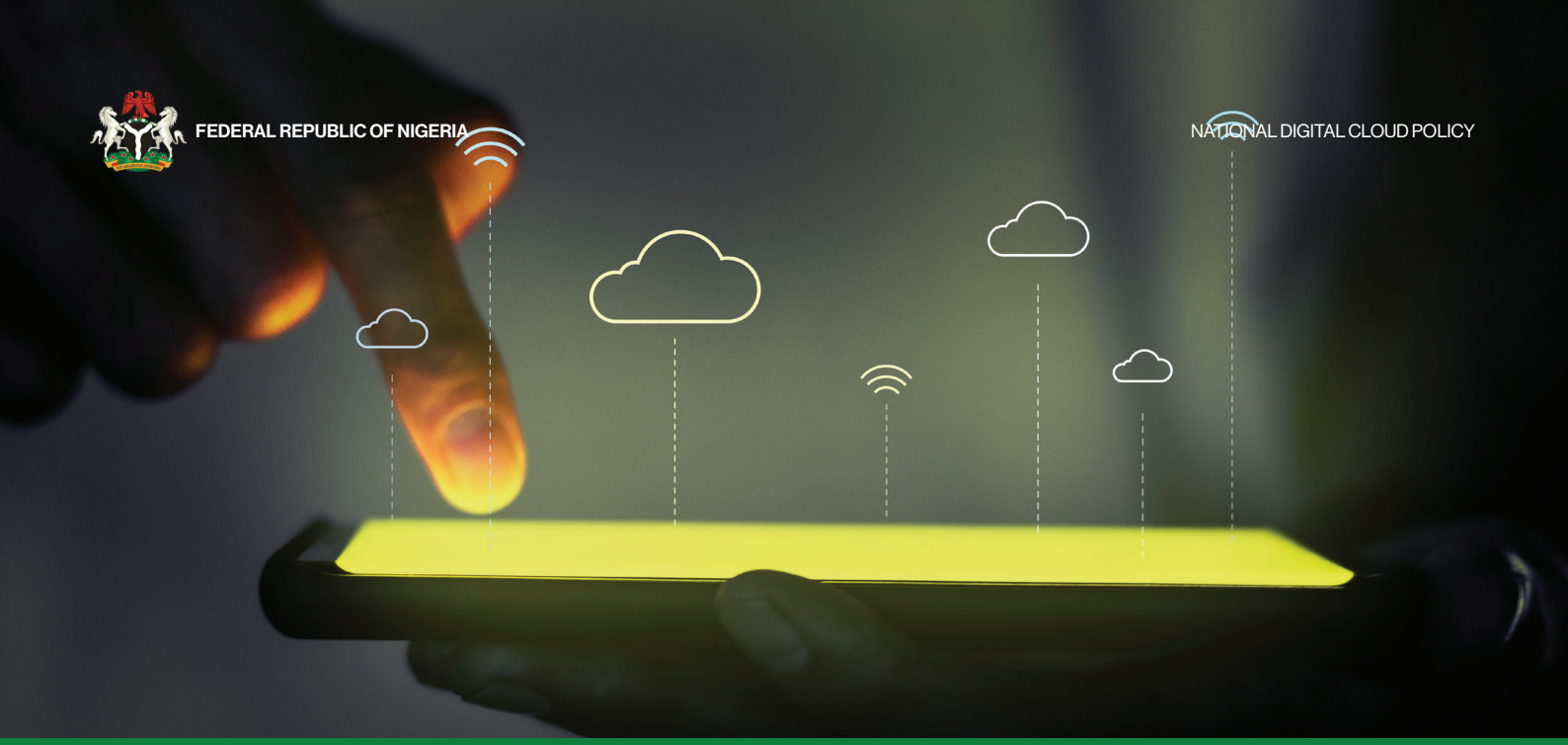
- All aggregated arrangements will be governed by framework agreements with enforceable Service Level Agreements covering availability, performance, security, portability, exit, and remedies.
- GBB will operate a transparent cost recovery and chargeback model, invoicing MDAs at published rates that pass through negotiated savings while sustaining operational viability.
- Payment assurance mechanisms, including standing payment arrangements and, where appropriate, escrow, will ensure that providers are paid reliably, preserving the credibility of the government as an anchor buyer. Unreliable payment would undermine the demand signal on which Part 3.3 depends.
- NITDA, BPP, GBB, and the Federal Ministry of Finance will jointly govern the framework through the Sovereign Government Cloud Governance Committee established under Part 12.7, and will report utilisation, savings realised, and commitment coverage under Part 14.

10.5 Support for State Governments and Subnational Entities

While Part II binds Federal MDAs, its benefits extend to States, the Federal Capital Territory, and Local Governments on a voluntary, cooperative basis.

- Negotiated rates. States may opt in to framework agreements and negotiated rates, procuring services from registered providers at aggregated pricing without conducting separate negotiations.
- Anchor capacity. Capacity secured under federal anchor arrangements may be made available to participating states at predictable cost.
- Shared services. Participating states will be supported in adopting shared platforms and integrating with Federal Government data platforms or systems.
- Onboarding and skills. GBB will provide structured onboarding, advisory, and migration support, and state personnel will be eligible for training and certification under Part 6.
- Governance. NITDA will issue guidance on subnational participation, covering compliance, classification alignment, and cost recovery arrangements.

Subnational participation multiplies aggregated demand, further strengthening the negotiating position of government and the demand signal available to investors, while extending the pricing and service benefits of this Policy to all tiers of government.



PART III:

Sovereignty for Government And Regulated Data

11. Sovereignty Framework for Government and Regulated Data

11.1 Purpose and Justification

The preceding Parts establish an open, investment-led market. This Part addresses the narrow category of data where that openness must be qualified by national control.

The justification is specific rather than general. Where data records the operation of the state itself, where its compromise would prejudice national security, or where it is generated under a licence or regulatory obligation and its integrity underpins a critical national system, the government requires assured legal and operational control. That control cannot be secured by contract alone when the infrastructure that holds the data is subject to a foreign jurisdiction whose legal processes may compel disclosure or whose commercial or political decisions may interrupt service, without effective recourse under Nigerian law.

Sovereignty requirements under this Part are therefore justified by identified risk to identified national interests. They are not a general preference for domestic hosting, nor an instrument of industrial policy. Industrial development is pursued through the incentives in Part I, which operate by making Nigeria attractive rather than by making alternatives unlawful.

Consistent with that justification, requirements under this Part are constrained by the following principles:

- **Proportionality:** Requirements are calibrated to the data's sensitivity, and the most restrictive requirements apply only to the most sensitive category.
- **Specificity:** Requirements attach to defined categories of data, not to sectors, providers, or nationalities.
- **Transparency:** Classification criteria and residency requirements are published, and their application to particular categories of data is reviewable.
- **Periodic review:** Requirements are reviewed against changing risk and changing domestic capability, and relaxed where the original justification no longer holds.
- **Least restriction:** Where a control objective can be achieved by encryption, key custody, contractual safeguard, or audit rather than by physical residency, the less restrictive measure is preferred.
- **Economic assessment:** The anticipated effects of any restriction on investment, assessed before it is imposed.

11.2 Sovereign Data Defined

For this Policy, sovereign data means data that is:

- generated by the Federal Government of Nigeria, its Ministries, Departments and Agencies, or any entity exercising public functions on its behalf; or
- generated in accordance with regulations, licences, permits, concessions, partnerships, or directives issued by the Federal Government of Nigeria, including data produced by regulated entities, licensees, and government partners in the course of discharging obligations arising from such instruments, and designated as sovereign data in accordance with Part 11.6.

Data outside this definition is not subject to this Part. Its treatment is governed by the Nigeria Data Protection Act 2023,[16] applicable sectoral regulation, and ordinary commercial law. Nothing in this Part restricts the hosting or processing of commercial data outside the scope of the definition.

[16] Nigeria Data Protection Act 2023, Laws of the Federation of Nigeri

11.3 Classification Framework

Sovereign data is classified into four levels. Hosting requirements attach to classification rather than to data type, sector, or provider identity, so that identical protections apply to identical risk regardless of which institution holds the data.

Level	Category	Description	Hosting Requirement
Level 4	Classified	Data relating to national security, defence, critical infrastructure, or information whose compromise could threaten national stability or security	Hosted exclusively on infrastructure physically located in Nigeria under sovereign control, with processing within Nigerian jurisdiction
Level 3	Highly Sensitive	Sensitive personal data, regulated data including financial, health, biometric, and identity data, and other data protected under applicable law	Stored in Nigeria at rest, with continuous sovereign recovery capability; processing in approved environments subject to safeguards
Level 2	Sensitive	Internal government operational data, administrative records, and data that could cause moderate risk if disclosed'	May be deployed in hybrid environments, including approved international infrastructure, subject to prior authorisation
Level 1	Open	Data intended for public access, or low risk information with minimal impact if disclosed	May be hosted on any compliant infrastructure without residency restriction

Classification determines treatment. Where a dataset contains elements of more than one classification, the higher classification governs unless the elements are separable and separately controlled. Classification takes precedence over data type: the same category of information may attract different treatment depending on the context in which it is held and the consequence of its compromise.

Each MDA shall be responsible for ensuring that datasets under its custody are classified by authorised personnel using the published classification criteria. Classification decisions shall be documented, reviewable and periodically reassessed. Where datasets are shared or combined, the applicable classification shall be determined in accordance with the highest applicable risk unless the data elements are demonstrably separable and separately controlled.

11.4 Residency and Control Requirements

- Level 4 workloads must be hosted on infrastructure physically located in Nigeria, with processing occurring within Nigerian jurisdiction and encryption keys generated and held in Nigeria under government control.
- Level 3 workloads must be stored at rest in Nigeria, with a continuously recoverable copy maintained there. Processing may occur in approved environments subject to regulatory approval, encryption controls, and enforceable contractual safeguards.
- Level 2 workloads may be deployed in hybrid environments. Placement outside Nigeria requires prior authorisation from NITDA under the National Cloud Guideline 2026.
- Level 1 workloads are not subject to residency requirements.
- For Level 4 and Level 3 workloads, the recovery copy must be maintained at a facility located geographically separate from the primary site, in accordance with Part 5.2.
- Residency requirements apply to the data, not to the provider. A provider of any nationality may host sovereign data provided the infrastructure and controls meet the applicable requirements.

11.5 Cross Border Processing

- Cross-border processing of sovereign data is permitted where expressly authorised under this Part, and must comply with the transfer safeguards of the Nigeria Data Protection Act 2023.[17]
- Authorisation is assessed against the adequacy of protection in the receiving jurisdiction, the sensitivity of the data, the availability of encryption and key custody arrangements, and the enforceability of contractual safeguards.
- The Nigeria Data Protection Commission, will publish and maintain the list of jurisdictions recognised as providing adequate protection, giving effect to Part 4.3.
- Authorisation decisions will be issued within published timeframes, refusals will state reasons, and determination performance will be reported under Part 14.
- Authorisations will be reviewed periodically and may be varied where circumstances in the receiving jurisdiction change materially.

11.6 Designation of Regulated Data as Sovereign Data

Data generated under regulation, licence, or directive becomes subject to this Part only upon designation. Designation is a deliberate act requiring justification, not an automatic consequence of regulatory status.

- A regulator or MDA seeking designation will submit a proposal to the Sovereign Government Cloud Governance Committee identifying the data category, the national interest at stake, the risk that the designation addresses, and the least restrictive measure capable of addressing it.
- The Committee will assess the proposal against the principles in Part 11.1, consult affected sectors and providers, and assess the anticipated compliance cost and market impact.
- Designations will specify the applicable classification level, take effect after a transition period sufficient to permit compliance, and be reviewed at intervals of no more than 3 years.
- A register of designations will be maintained and published by NITDA, so that regulated entities can ascertain their obligations from a single authoritative source.
- Designation may be revoked, and classification levels reduced, where the Committee determines that the original justification no longer holds.

[17] Nigerian Data Protection Act 2023, Laws of the Federation of Nigeria

The classification framework in Section 11.3 and the residency requirements in Section 11.4 take effect upon approval

11.7 Presidential Approval

Given the economic significance of residency requirements and their implications for Nigeria's trade position and investment climate, the sovereignty component of this Policy is subject to Presidential approval.

- The classification framework in Part 11.3 and the residency requirements in Part 11.4 take effect upon approval by the President of the Federal Republic of Nigeria, on the recommendation of the Federal Executive Council.
- Any designation under Part 11.6 that would apply Level 4 or Level 3 requirements to a category of regulated data requires Presidential approval, on the recommendation of the Federal Executive Council following assessment by the Sovereign Government Cloud Governance Committee.
- Any amendment that tightens the requirements in Part 11.3 or 11.4, or extends their application to additional categories of data, likewise requires Presidential approval.
- Relaxation of requirements, removal of a designation, or the grant of an individual authorisation under Part 11.5 does not require Presidential approval. NITDA may affect it on the Committee's recommendation.
- Submissions seeking Presidential approval must be accompanied by an assessment of the anticipated effect on investment, trade, and compliance costs, together with the Committee's opinion on proportionality and its record of consultation with affected sectors.

This requirement ensures that restrictions on data location are adopted deliberately, at the highest level of government, with their economic consequences expressly weighed. The asymmetry is intentional and favours. openness: relaxation is openness: relaxation is administratively straightforward, while restriction requires Presidential authority.

11.8 Security and Access Control

- Access to sovereign data will be governed by role-based access control, the principle of least privilege, and multi-factor authentication.
- Administrative access to Level 4 and Level 3 environments will be restricted to personnel vetted in accordance with applicable requirements.
- Encryption will be applied to sovereign data at rest and in transit, with key management arrangements appropriate to classification and, for Level 4, key custody within Nigeria under government control.
- Logging, monitoring, and audit capability will be maintained and made available for regulatory inspection.
- Security incidents affecting sovereign data will be notified in accordance with applicable requirements, and material breaches involving Level 4 or Level 3 data escalated under Part 12.5.

11.9 Portability and Interoperability Safeguards

- Sovereign data must remain portable, and providers must support documented export in non-proprietary formats.
- Architectures that create an exclusive dependency on a single provider for Level 4 or Level 3 workloads will be avoided.
- Exit assistance obligations will be contractually enforceable and tested periodically rather than assumed.
- Sovereign systems will interoperate through open standards and documented interfaces, supporting integrated service delivery across institutions.

11.10 Enforcement and Compliance

- NITDA will audit MDA and provider compliance with classification, residency, and hosting requirements, and may direct remediation, suspend deployments, or withhold ICT project clearance for non-compliant systems.
- Providers hosting sovereign data in breach of applicable requirements will be subject to remedial directives, sanctions, suspension, or revocation of registration.
- Material breaches involving Level 4 or Level 3 data will be escalated to ONSA and other competent authorities.
- Enforcement is a principal cause of the limited implementation of the 2019 policy: the absence of binding compliance consequences.

12. Institutional Roles and Governance for Sovereign Data

This Part consolidates the roles of the principal institutions regarding sovereign data. Their broader functions in relation to the wider market are addressed in Parts I and II.

12.1 Allocation of Functions

Three institutions hold distinct and non-overlapping functions:

- NITDA regulates, sets standards, registers providers, and authorises. It does not operate infrastructure.
- GBB operates, aggregates, and delivers cloud-based capacity. It does not regulate, and its operational role confers no supervisory authority over competing providers.
- BPP governs procurement compliance. It does not set technical standards.

Where functions intersect, the Sovereign Government Cloud Governance Committee resolves the allocation, and its determination is recorded and published.

Each institution shall exercise its functions within its statutory mandate. Where implementation requires joint action, the lead institution shall be identified in the applicable guideline, directive or implementation plan, with supporting institutions and deliverables clearly specified.

12.2 Galaxy Backbone Limited (GBB)

In line with Federal Government Circular dated 3rd November 2020,[18] GBB is the primary digital infrastructure provider of the Federal Government, operating under a dual mandate that combines delivery of shared government services with aggregation, optimisation, and commercialisation of cloud capacity across the public sector. In discharging this mandate, GBB is required to develop into a commercially disciplined and technically advanced State Owned Enterprise capable of operating to international standards.

In relation to sovereign data, GBB will:

- Operate as default host for Level 4 and Level 3 government workloads, maintaining infrastructure meeting the requirements of Part 11.4;
- Design, deploy, and operate shared government platforms and foundational services, including backup, disaster recovery, and security operations, architected across geographically separated sites;
- Aggregate government demand and negotiate framework agreements incorporating the safeguards required under this Part;
- Maintain encryption key custody arrangements for Level 4 workloads under government control;
- Guide workload classification, placement, and deployment model selection, including hybrid and multicloud architectures;
- Provide migration, onboarding, advisory, and deployment support to MDAs and participating states;
- Establish and enforce Service Level Agreements consistent with national requirements;
- Report utilisation, capacity, compliance, and service performance to the Sovereign Government Cloud Governance Committee.

[18] Federal Government Circular dated 3rd November 2020, reference No. 58541/T2/350, designating Galaxy Backbone Limited as the primary digital infrastructure provider of the Federal government.

12.3 GBB Institutional Development

To discharge the mandate in Part 12.2, GBB will implement a structured institutional development programme.

- **Organisational structuring:** GBB will establish Strategic Business Groups covering shared government services; cloud aggregation and commercial services; cloud engineering and operations; security and sovereign assurance; advisory and deployment support; and partnerships and ecosystem development. Special purpose vehicles or programme-specific structures may be established where required.
- **Internal capability:** GBB will build in-house expertise in multicloud architecture, platform engineering, cybersecurity, data infrastructure, commercial operations, and service delivery management.
- **Transitional arrangements:** In initial phases, GBB may enter co-delivery or managed service arrangements with qualified partners, including international providers, data centre operators, and system integrators, to accelerate deployment. Such arrangements must preserve GBB's authority over architecture, standards, and service outcomes, maintain sovereign control over data and systems, and embed knowledge transfer as a core requirement.
- **Sunset provisions:** Transitional arrangements are capability-building mechanisms rather than permanent dependencies. Each will include defined sunset provisions, performance benchmarks, capability transfer requirements, and transition plans. No capability required for sovereign cloud operations should remain permanently outsourced where it can reasonably be developed within GBB.

12.4 National Information Technology Development Agency (NITDA)

NITDA is the principal policy, regulatory, and standards authority for cloud adoption, and the regulator for sovereign data. NITDA will:

- Issue and maintain the classification framework, residency standards, and technical guidance giving effect to this Part;
- Administer the Digital Infrastructure Assurance Registration scheme, registering providers and issuing Certificates of Registration in the applicable class;
- Determine applications for cross-border processing authorisation under Part 11.5 and for exemptions under Part 7.2 and 8.2;
- Maintain and publish the register of designations under Part 11.6 and the list of recognised jurisdictions under Part 11.5;
- Issue rules governing the National Digital Marketplace jointly with BPP and GBB;
- Audit MDA and provider compliance, and direct remediation, suspend deployments, or withhold ICT project clearance where requirements are not met;
- Recommend sanctions, suspension, or revocation of registration in respect of providers in material breach;
- Administer ICT project clearance consistently with this Policy;
- Establish mechanisms for continuous compliance monitoring to promote preventive assurance rather than purely reactive enforcement.

12.5 Office of the National Security Adviser (ONSA)

- ONSA will advise on the classification and treatment of Level 4 workloads and on exemptions sought on national security grounds.
- Material breaches involving Level 4 or Level 3 data will be escalated to ONSA and other competent authorities.
- ONSA will participate in the security and risk assessment under Part 14.3.

12.6 Bureau of Public Procurement (BPP)

BPP governs the procurement dimension of sovereign data arrangements. BPP will:

- Ensure that procurement of services involving sovereign data conforms to public procurement law and to this Policy;
- Issue and maintain standard contractual provisions incorporating the safeguards required under Part 9.4 and 11.9;
- Govern procurement compliance within the National Digital Marketplace, jointly with NITDA and GBB;
- Monitor for duplicative or uncoordinated acquisition of services involving sovereign data;
- Ensure that procurement processes remain open, competitive, and non-discriminatory consistent with Part 4.6.

12.7 Sovereign Government Cloud Governance Committee

A Sovereign Government Cloud Governance Committee is established as a standing committee to provide strategic oversight, policy coordination, and whole-of-government governance for the implementation and continuous development of this Part.

The Honourable Minister responsible for Communications, Innovation and Digital Economy will serve as Chairman. The Director General and Chief Executive Officer of NITDA will serve as Alternate Chairman and may preside in the absence of the Chairman or upon the Chairman's delegation. NITDA will serve as Secretariat and provide technical, administrative, and coordination support.

Membership will comprise appropriately senior representatives of:

- Federal Ministry of Communications, Innovation and Digital Economy;
- Federal Ministry of Finance;
- Federal Ministry of Agriculture & Food Security;
- Federal Ministry of Health & Social Development;
- Federal Ministry of Education;
- Federal Ministry of Justice;
- National Information Technology Development Agency;
- National Identity Management Commission;
- Bureau of Public Procurement;
- Office of the National Security Adviser;
- Nigeria Data Protection Commission;
- Office of the Secretary to the Government of the Federation;
- Office of the Head of the Civil Service of the Federation;
- Office of the Accountant General of the Federation;
- Budget Office of the Federation;
- Central Bank of Nigeria;
- Galaxy Backbone Limited; and
- such other Federal Public Institutions as the Chairman may determine.

The Committee may co-opt sector regulators and, for matters affecting the market, industry representatives.

Without prejudice to the statutory mandates of relevant institutions, the Committee will:

- provide strategic direction and oversight for implementation of this Part;
- assess designation proposals under Part 11.6 and advise on proportionality;
- prepare submissions seeking Presidential approval under Part 11.7, including the required economic assessment;
- review classification and residency requirements periodically against changing risk and domestic capability;

- review classification and residency requirements periodically against changing risk and domestic capability;
- coordinate institutions to ensure a consistent whole of government approach to cloud adoption and migration;
- provide oversight for the classification and placement of government systems, data, and workloads;
- promote consolidation and shared use of government infrastructure, including common platforms, backup, and disaster recovery;
- review government-wide adoption, utilisation, and expenditure and recommend measures to improve efficiency and value for money;
- promote common requirements for procurement, portability, interoperability, business continuity, service levels, and exit arrangements;
- identify systemic risks and implementation barriers and coordinate responses;
- resolve questions of functional allocation arising under Part 12.1;
- facilitate collaboration among government institutions and, where appropriate, the private sector and academia;
- maintain an annual work programme and implementation dashboard and shall record decisions on functional allocation and publish appropriate non-sensitive outcomes. and
- report to the Federal Executive Council on implementation, compliance, and market impact.

PART IV:

Implementation and Review

13. Implementation Roadmap

13.1 Phase 1: Activation and Baseline (0 to 6 Months)

- Publication of this Policy and issuance of implementing directives;
- Submission of the sovereignty component for Presidential approval under Part 11.7;
- Establishment of the Sovereign Government Cloud Governance Committee;
- Baseline audit of MDA systems, workloads, expenditure, and skills, conducted jointly with the data inventory required under the National Cloud Guideline 2026 to avoid duplicative exercises;
- Publication of incentive qualification criteria under Part 3.8 and issuance of fiscal implementation guidance under Part 3.2;
- Establishment of the Anchor Capacity Fund and issuance of budget circular guidance under Part 10.1;
- Establishment of the coordinated investment facilitation point under Part 3.4;
- Publication of baseline values for the indicators in Part 14.4.

13.2 Phase 2: Deployment and Market Activation (6 to 12 Months)

- Operationalisation of the National Digital Marketplace and onboarding of registered providers;
- Conclusion of initial anchor offtake agreements and framework agreements;
- Commencement of priority MDA migrations;
- Publication of the list of recognised jurisdictions under Part 11.5;
- Initiation of structured capacity development and certification programmes under Part 6;
- Commencement of regional market development activity under Part 4;
- First reporting on incentive uptake and investment committed.

13.3 Phase 3: Scale and Export Development (12 to 24 Months)

- Scaling of migration across MDAs and onboarding of participating states;
- Expansion of contracted capacity and formalisation of marketplace operations;
- Regional interconnection and peering development under Part 5.3;
- Pursuit of mutual recognition arrangements under Part 4.4;
- First periodic review of classification and residency requirements under Part 11.1;
- Reporting of export performance under Part 14;
- Assessment of incentive effectiveness under Part 3.9.

13.4 Implementation Governance

- NITDA will provide regulatory oversight and standards enforcement;
- GBB will lead operational delivery and aggregation;
- BPP will ensure alignment and compliance in procurement;
- The Federal Ministry of Finance and the Budget Office will provide funding oversight;
- MDAs will be responsible for adoption and execution within their respective domains;
- Where an implementation activity depends on the establishment of a funding, regulatory or institutional mechanism, the responsible institution shall report the status of that dependency through the annual implementation report.
- The Sovereign Government Cloud Governance Committee will coordinate across institutions and report to the Federal Executive Council.

14. Monitoring, Evaluation and Review

14.1 Performance Monitoring and Reporting

- NITDA will monitor implementation and publish an annual implementation report.
- GBB will report on capacity, utilisation, savings realised, and service performance.
- MDAs will report on migration progress, classification coverage, and expenditure.
- Reporting will distinguish outcomes attributable to this Policy from those attributable to underlying market growth, enabling assessment of policy effectiveness.

14.2 Policy Review

- This Policy will be reviewed annually, and comprehensively at intervals not exceeding three years.
- The review will assess investment attracted, installed capacity, export performance, government savings achieved, incentive effectiveness, and the continuing proportionality of requirements under Part III.
- Review findings will be reported to the Federal Executive Council with recommendations.

14.3 Market, Security and Risk Assessment

- NITDA will monitor market concentration, competitive conditions, and pricing, and will report where market structure threatens the contestability this Policy seeks to maintain.
- Security and resilience risks will be assessed in consultation with ONSA and relevant authorities.
- Assessment findings will inform review under Part 14.2.

14.4 Key Performance Indicators

Implementation will be tracked against the following indicators, measured from the baseline in Part 1.7. NITDA will publish baseline values within six months of adoption and report progress annually. Targets are indicative and will be validated against the Phase 1 baseline audit.

KPI	Target (12 Months)	Target (24 Months)	Lead
Private investment committed to cloud and data infrastructure in Nigeria	USD 250m	USD 750m	NITDA / Ministry of Finance
Installed compliant hosting capacity (net IT load)	2 MW	5 MW	GBB / NITDA
Capacity contracted to customers outside Nigeria	Baseline established	10% of installed capacity	NITDA / NEPC
Export earnings from cloud and data services	Baseline established	Measurable growth	NITDA / NEPC

Registered providers listed on the National Digital Marketplace	10	25	NITDA / BPP
Median time to determine investment facilitation applications	Published standard met	Sustained	NITDA
New government systems designed cloud first (ICT clearance data)	70%	95%	NITDA
Eligible existing MDA workloads migrated	15%	40%	MDAs / GBB
Savings from aggregated and negotiated procurement	15% or more	25% or more	GBB / BPP
MDAs with dedicated cloud budget lines	50%	100%	Budget Office / MDAs
Government systems with documented data classification	60%	100%	MDAs / NITDA
Personnel certified under the national cloud competency framework	2,500	10,000	NITDA / DBI
Hosting capacity located outside Lagos	Baseline established	Measurable growth	NITDA
Level 4 and Level 3 workloads with geographically separated recovery	50%	100%	GBB / MDAs
Average PUE of newly registered facilities	1.6 or below	1.5 or below	NITDA
Median time to determine cross-border authorisation applications	Published standard met	Sustained	NITDA
States participating in the aggregation framework	3	10	GBB / NITDA

14.5 Policy Position

This Policy supersedes the Nigeria Cloud Computing Policy 2019[19] and constitutes the Federal Government's framework for cloud investment, trade, government adoption, and the sovereignty of government and regulated data. It is read together with the Nigeria Data Protection Act 2023 and the Cybercrimes (Prohibition, Prevention, etc.). Amendment Act 2024, the NITDA Act 2007,[20] and applicable national security directives.

The National Cloud Guideline 2026, the National Cloud Technical Guideline 2026, and the National Digital Infrastructure Assurance Framework are implementing instruments of this Policy. In the event of conflict concerning matters within its scope, this Policy prevails, and NITDA will amend the relevant instrument accordingly.

Part III takes effect upon Presidential approval in accordance with Part 11.7. Parts I, II, and IV take effect upon publication.

[19] Nigeria Cloud Computing Policy 2019, which introduced the Cloud First principle for Federal Public Institutions.
[20] Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024; National Information Technology Development Agency Act 2007.

FEDERAL REPUBLIC
OF NIGERIA