# Government Network Infrastructure Baseline and Audit Guideline for Federal Public Institutions

March 2026

## TABLE OF CONTENTS

## 1. Explanatory Note

This Guideline is issued to establish a **uniform technical baseline and audit framework** for network infrastructure deployed across Federal Public Institutions (FPIs).

The increasing reliance of government institutions on digital platforms, interconnected networks, and data-driven services has made **secure, resilient, and auditable network infrastructure** a critical requirement for effective public service delivery.

This Guideline therefore provides:

a. A **clear and objective basis** for auditing existing government network infrastructure;

b. **Minimum technical requirements** for validating future network procurements subject to IT Project Clearance; and

c. A **tier-aware but non-discretionary framework** that ensures proportional treatment of institutions based on operational criticality, without weakening baseline security and interoperability obligations.

The Guideline is designed to be **self-executing**, using binary and quantitative criteria, and does not require supplementary standard operating procedures for implementation.

## 2. Authority

This Guideline is issued pursuant to the powers conferred on the **National Information Technology Development Agency** under the **National Information Technology Development Agency (NITDA) Act, 2007**, including but not limited to provisions that empower the Agency to:

a. Develop and issue standards, guidelines, and frameworks for the regulation, coordination, and development of information technology systems in Nigeria;
b. Provide regulatory oversight for the planning, acquisition, deployment, and utilisation of information technology resources within Federal Public Institutions; and
c. Establish mechanisms to ensure the security, interoperability, efficiency, and sustainability of government IT infrastructure.

## 3. Commencement

This Guideline shall **come into effect on the date of its issuance by NITDA**, unless otherwise specified, and shall apply to:

a. All **existing network infrastructure** within Federal Public Institutions, subject to audit in accordance with this Guideline; and
b. All **future network-related procurements**, upgrades, or expansions, subject to validation through the **NITDA IT Project Clearance** process.

## 4. Application and Scope

### Application

This Guideline applies to:

a. All **Federal Public Institutions (FPIs)**, including Ministries, Departments, Agencies, and other government bodies that deploy, operate, or manage network infrastructure; and
b. All **network infrastructure assets**, whether owned, leased, outsourced, cloud-enabled, or otherwise deployed for the delivery of government services.

### Scope

The scope of this Guideline covers:

a. The **audit of existing government network infrastructure** to determine compliance with defined minimum technical requirements;
b. The establishment of **mandatory minimum technical requirements** for network-related procurements, upgrades, or expansions, subject to **NITDA IT Project Clearance**;
c. A **tier-aware classification framework** for contextualising audit results based on institutional criticality and scale; and
d. The documentation, reporting, and interpretation of audit outcomes for regulatory and oversight purposes.

This Guideline does **not** prescribe vendor-specific solutions, detailed network architectures, or operational procedures beyond what is required to establish auditability and baseline compliance.

## 5. Definitions

In this Guideline, unless the context otherwise requires:

**Agency** means the **National Information Technology Development Agency (NITDA)**.

**Audit** means a structured assessment conducted using binary and quantitative criteria to determine compliance with this Guideline.

**Federal Public Institution (FPI)** means any ministry, department, agency, or government entity funded or operated by the Federal Government of Nigeria.

**IT Project Clearance** means the mandatory review and validation process administered by NITDA for government IT projects and procurements.

**Minimum Technical Requirements** means the lowest acceptable technical specifications that network infrastructure must meet to be considered compliant under this Guideline.

**Network Infrastructure** includes routers, switches, firewalls, wireless access points, monitoring tools, and associated systems used to enable connectivity, security, and data transmission.

**Tier Classification** means the categorisation of FPIs based on measurable indicators of digital dependence, service criticality, and operational risk.

## 6. Objectives

The objectives of this Guideline are to:

a. Establish a **uniform and auditable baseline** for network infrastructure deployed across Federal Public Institutions;

b. Ensure that government network infrastructure is **secure, resilient, interoperable, and fit for purpose**;

c. Provide a **clear and objective basis** for auditing existing network assets using binary and quantitative criteria;

d. Support **sound IT procurement decisions** by defining minimum technical requirements applicable to future network investments;

e. Enable **risk-proportionate oversight** through tier-based contextualisation without weakening baseline compliance; and

f. Strengthen NITDA's role in **protecting government IT investments** and ensuring continuity of public service delivery.

## PART I – GENERAL PROVISIONS

1. This Guideline is issued by the National Information Technology Development Agency (NITDA) pursuant to its statutory mandate and shall serve as a **binding regulatory instrument** for all Federal Public Institutions to which it applies. Compliance with this Guideline shall be required for:
   a. the audit of existing government network infrastructure; and
   b. the validation of future network-related procurements through the IT Project Clearance process.

2. This Guideline shall be applied in conjunction with:
   a. NITDA IT Project Clearance requirements;
   b. Applicable public procurement laws and regulations; and
   c. Other relevant government IT regulatory instruments issued by NITDA.

3. Where any conflict arises between this Guideline and another government instrument, the provisions of this Guideline shall prevail **to the extent of network infrastructure audit and minimum technical requirements**.

4. All requirements expressed using the word **“shall”** in this Guideline are **mandatory**.

5. Requirements expressed using the word **“may”** are optional and do not affect compliance status.

6. Compliance shall be determined strictly on the basis of:
   a. objective audit results; and
   b. documented evidence recorded in accordance with this Guideline.

7. This Guideline shall be interpreted to:
   a. promote secure, resilient, and interoperable government network infrastructure;
   b. support proportional oversight based on institutional criticality; and
   c. avoid subjective or discretionary application.

8. Nothing in this Guideline shall be interpreted as:

   a. prescribing specific vendors or proprietary technologies; or
   b. replacing internal operational procedures of FPIs beyond audit and minimum baseline requirements.

9. Existing network infrastructure deployed within Federal Public Institutions shall be subject to audit in accordance with this Guideline.

10. All future network-related procurements, upgrades, or expansions shall:

    a. comply with the minimum technical requirements defined in this Guideline; and
    b. be subject to validation through NITDA IT Project Clearance prior to implementation.

## PART II – TIER CLASSIFICATION FRAMEWORK

1. The Tier Classification Framework is established to provide a **structured and objective basis** for contextualising network infrastructure audit results across Federal Public Institutions.

2. Tier classification is intended to reflect differences in:

   a. scale of operations;
   b. digital service dependency;
   c. data sensitivity; and
   d. operational and national risk exposure.

3. Tier classification shall be used solely for **interpretation, prioritisation, and risk contextualisation** and shall not be applied to waive, relax, or substitute any minimum technical requirement under this Guideline.

4. Tier classification shall be determined using **observable and measurable characteristics** of an institution at the time of audit.

5. Classification shall be based on the **highest applicable criterion met** by the institution.

6. No discretionary judgement, subjective assessment, or self-declaration by an institution shall be used to determine tier status.

### Tier Definitions and Criteria

### Tier 1: Low-IT Usage Institutions

7. An institution shall be classified as **Tier 1** where **all** of the following apply:

   a. fewer than two hundred (200) active users;
   b. typical network traffic below five hundred megabits per second (500 Mbps);
   c. digital services are primarily internal and non-mission-critical;

d. no national or high-availability public-facing platforms are operated; and
e. limited data sensitivity, excluding large-scale personal, financial, or security-related data.

**Illustrative services** under Tier 1 include:
a. internal email and collaboration systems;
b. basic document management and records systems; and
c. informational websites without transactional functionality.

### Tier 2: Moderate-IT Usage Institutions

8. An institution shall be classified as **Tier 2** where **any** of the following apply:
a. between two hundred (200) and two thousand (2,000) active users;
b. network traffic between five hundred megabits per second (500 Mbps) and five gigabits per second (5 Gbps);
c. operation of public-facing digital services that are not nationally mission-critical;
d. multi-site or branch connectivity requiring wide area networking; or
e. processing of data requiring enhanced security controls.

**Illustrative services** under Tier 2 include:
a. public portals for applications, registrations, or submissions;
b. internal finance, procurement, or grant-management systems; and
c. sectoral education or health platforms with limited real-time dependency.

### Tier 3: High-IT / Mission-Critical Institutions

9. An institution shall be classified as **Tier 3** where **any** of the following apply:
a. more than two thousand (2,000) users or nationwide digital service reach;
b. network traffic equal to or exceeding five gigabits per second (≥ 5 Gbps);
c. operation of national, mission-critical, or high-availability platforms;
d. processing of high-risk or regulated data at scale; or
e. requirement for continuous twenty-four-hour (24/7) service availability.

**Illustrative services** under Tier 3 include:
a. national identity, immigration, customs, or border-management systems;
b. government payment, revenue, or financial settlement platforms;

c. nationwide health, education, or social service platforms; and
d. security, law-enforcement, intelligence, or emergency-response systems.

## Tier Assignment Rules

10. Tier classification shall reflect the **current operational state** of an institution and not planned or aspirational upgrades.

11. Where an institution meets criteria across multiple tiers, the **highest applicable tier shall apply**.

12. Tier classification shall be reviewed:

a. during each audit cycle; or
b. following any material change in network infrastructure or service criticality.

13. Notwithstanding the numerical criteria relating to user population or network traffic, any Federal Public Institution that operates digital services whose characteristics correspond to those described under Tier 2 or Tier 3 shall be automatically classified in the applicable higher tier.
14. Such classification shall apply where the institution operates **public-**facing, citizen-facing, or mission-critical digital platforms, including systems supporting national registries, licensing, payments, security operations, or other essential government services.
15. In such circumstances, the tier classification shall be determined by the operational criticality of the service rather than the size of the institution**.**

## Application of Tier Classification

16. Tier classification shall be applied to:
a. contextualise audit findings and compliance scores;
b. prioritise remediation sequencing and upgrade urgency; and
c. support risk-based oversight and reporting.

17. Tier classification shall **not** be used to:

a. reduce audit scope;
b. alter compliance thresholds; or
c. waive minimum technical baseline requirements.

### Relationship with Tier-Based Requirements

18. Additional tier-conditioned minimum requirements are specified in **Annex C (Annex 3)** to this Guideline.

19. Such tier-based requirements shall apply **in addition to**, and not in replacement of, the baseline requirements set out in Part IV.

### Tier-Based Network Architecture Requirements

20. Federal Public Institutions shall design and operate their network infrastructure in accordance with **minimum architecture and resilience controls appropriate to their Tier Classification**.
21. These controls are intended to ensure that network infrastructure deployed within Federal Public Institutions supports:

    a. secure segmentation of network environments;
    b. isolation of administrative management networks;
    c. protection of public-facing services through controlled security zones; and
    d. resilience against infrastructure or connectivity failures.

22. The **minimum architecture and resilience controls applicable to each tier are provided in Annex D of this Guideline**.
23. Institutions shall ensure that network infrastructure procured or deployed pursuant to this Guideline is integrated within architectures that comply with **Annex D requirements**.

## PART III – NETWORK INFRASTRUCTURE AUDIT FRAMEWORK

### Establishment of the Network Infrastructure Audit Framework

1. A Network Infrastructure Audit Framework is hereby established for the purpose of assessing compliance with this Guideline across Federal Public Institutions.

2. The audit framework shall apply to:

   a. existing network infrastructure deployed within Federal Public Institutions; and
   b. network infrastructure proposed for procurement, upgrade, or expansion and subject to NITDA IT Project Clearance.

### Architecture and Resilience Verification

1. Network infrastructure audits conducted under this Guideline shall include verification of network architecture and resilience controls implemented by Federal Public Institutions.
2. The audit shall confirm that the institution’s network infrastructure incorporates the minimum segmentation, management isolation, and redundancy mechanisms specified in **Annex D**.
3. Verification shall be conducted using the Network Audit Checklist provided in **Annex A**.
4. Where architecture controls required under **Annex D** are not implemented, the institution shall be deemed non-compliant with the relevant provisions of this Guideline.

**Audit Methodology**

3. Audits conducted under this Guideline shall be executed using **objective, deterministic criteria only**.

4. Each audit item shall be assessed using either:

   a. a **binary outcome** (Yes / No); or
   b. a **quantitative measurement** against a defined minimum threshold.

5. Subjective judgement, narrative scoring, maturity interpretation, or discretionary assessment shall not be applied.

**Audit Structure**

6. Audits shall be conducted by assessing network infrastructure assets against the minimum technical requirements set out in **Part IV** and applicable tier-based requirements in **Annex C**.

7. Audit assessments shall be recorded using the **Network Audit Checklist** contained in **Annex A**.

8. Each audit entry shall include:

   a. the asset category and identifier;
   b. the audit parameter assessed;
   c. the recorded result (Yes / No or numeric value); and
   d. a reference to supporting evidence.

**Evidence Requirements**

9. All audit results shall be supported by verifiable evidence.

10. Acceptable forms of evidence include:

a. configuration outputs or command-line extracts;
b. original equipment manufacturer (OEM) technical documentation or datasheets;
c. monitoring system outputs or screenshots;
d. system logs or retention records; or
e. physical inspection records, where applicable.

11. Evidence shall be directly traceable to the asset assessed.

12. Audit items without supporting evidence shall be recorded as **non-compliant**.

### Audit Outcomes

13. Audit outcomes shall be determined automatically based on recorded results, as follows:
a. **Compliant**, where all applicable requirements are met;
b. **Partially Compliant**, where one or more non-critical requirements are unmet; or
c. **Non-Compliant**, where one or more critical requirements are unmet or evidence is unavailable.

14. Audit outcome determination shall not require additional validation, interpretation, or discretionary approval.

### Compliance Scoring

15. Compliance with this Guideline shall be determined through the combined assessment of:
a. the minimum infrastructure requirements defined in **Part IV**;
b. audit results recorded using the **Network Audit Checklist in Annex A**;
c. compliance scoring under **Annex B**;
d. tier-based requirements specified in **Annex C**; and
e. architecture and resilience controls specified in **Annex D**.

### Repeatability and Consistency

16. The audit framework shall be applied consistently across:
a. all Federal Public Institutions;
b. different audit cycles; and
c. audits conducted by different assessors.

17. Audit results shall be reproducible when the same assets are assessed under the same conditions.

### Relationship with IT Project Clearance

18. Audit results generated under this Part may be used to:
    a. establish baseline compliance status; and
    b. inform technical validation under the **NITDA IT Project Clearance** process.

19. Future network procurements shall demonstrate alignment with the minimum technical requirements validated through this audit framework.

## PART IV – MINIMUM TECHNICAL BASELINE REQUIREMENTS

### General Baseline Obligations

1. All Federal Public Institutions shall ensure that network infrastructure deployed or procured complies with the **minimum technical baseline requirements** specified in this Part.

2. The minimum technical baseline requirements apply to:

    a. existing network infrastructure, subject to audit under this Guideline; and
    b. future network-related procurements, upgrades, or expansions subject to **NITDA IT Project Clearance**.

3. Minimum technical baseline requirements are **mandatory** and shall not be waived, reduced, or substituted by internal policies, vendor assurances, or contractual arrangements.

4. Where additional tier-based minimum requirements apply, such requirements shall be enforced in accordance with **Annex C and D**.

### Core Network Infrastructure Requirements

5. Core routers deployed within Federal Public Institutions shall meet the following minimum requirements:
    a. minimum forwarding capacity of not less than 1 gigabit per second (≥ 1 Gbps) for Tier 1 institutions and not less than 10 gigabits per second (≥ 10 Gbps) for Tier 2 and Tier 3 institutions;
    b. support for **IPv6, OSPF, BGP, MPLS, and redundancy protocols**;
    c. dual, hot-swappable power supplies;
    d. redundant route processors with non-stop forwarding capability;
    e. hardware-based encryption of **AES-256 or higher**;
    f. secure boot and digitally signed firmware;
    g. role-based access control for administrative functions;

h. application-aware quality of service and policy-based routing; and
i. architectural design capable of achieving **minimum availability of 99.99 percent**.

6. Tier-conditioned enhancements to core infrastructure shall apply as specified in **Annex C**.

### Edge Routing and Network Security Requirements

7. Edge routers and next-generation firewalls shall meet the following minimum requirements:
   a. routing and inspection capacity of **not less than 2.5 Gbps**;
   b. enabled **deep packet inspection, intrusion prevention or detection, application control, anti-malware, and web filtering**;
   c. support for **IPsec and SSL/TLS** with hardware-accelerated encryption throughput of **not less than 1 Gbps**;
   d. high-availability configuration supporting active-active or active-passive clustering;
   e. automated failover with recovery time **not exceeding five (5) seconds**; and
   f. centralised logging and telemetry using **syslog and NetFlow/IPFIX**, with secure export to monitoring or security systems.

8. Tier-based requirements for enhanced availability, monitoring, and integration shall apply as specified in **Annex C**.

### Switching Infrastructure Requirements

9. Switching infrastructure shall meet the following minimum requirements:
   a. access switches providing **Layer 2 Gigabit Ethernet** capability;
   b. distribution and core switches supporting Layer 3 switching with uplink capacity of not less than 1 Gbps for Tier 1 institutions and not less than 10 Gbps for Tier 2 and Tier 3 institutions, or higher where required to support operational demand.;
   c. minimum port density of **twenty-four (24) ports**;
   d. power over Ethernet support (**IEEE 802.3af/at/bt**) where required;
   e. support for **VLANs, QoS, LACP, and spanning tree protocols**;
   f. network access control using **IEEE 802.1X**, port security, and MAC filtering; and

g. secure management interfaces supporting **SSH and SNMPv3**, with automated configuration backup.

10. Tier-conditioned switching requirements shall apply as specified in **Annex C**.

### Wireless Network Infrastructure Requirements

11. Wireless access infrastructure shall meet the following minimum requirements:

    a. compliance with **Wi-Fi 6 (IEEE 802.11ax)** standard or higher;
    b. operation on **2.4 GHz and 5 GHz** frequency bands;
    c. support for **not fewer than fifty (50) concurrent clients per access point**;
    d. minimum aggregate throughput of **not less than 1.5 Gbps**;
    e. **WPA3** encryption with VLAN segmentation and centralised authentication using **RADIUS or IEEE 802.1X**;
    f. centralised wireless controller (cloud-based or on-premises); and
    g. minimum enclosure protection rating of **IP54**.

12. Additional wireless requirements based on tier classification shall apply as specified in **Annex C**.

### Network Monitoring and Visibility Requirements

13. All Federal Public Institutions shall deploy network monitoring and visibility tools that provide:
    a. a unified dashboard for network health, security, and bandwidth utilisation;
    b. support for **SNMPv3, syslog, and NetFlow/IPFIX**;
    c. threshold-based alerts for performance and security events;
    d. predictive indicators for capacity planning; and
    e. log retention for a minimum period of **twelve (12) months**.

14. Requirements for centralised monitoring, national visibility, and continuous operations shall apply based on tier classification in **Annex C**.

### Energy Efficiency, Support, and Lifecycle Requirements

15. Network equipment shall:
    a. comply with **Energy Star 8.0** or equivalent energy-efficiency certification;
    b. support low-power or energy-saving operational modes;
    c. comply with **RoHS and WEEE** environmental standards; and

d. operate within temperature range of **0°C to 45°C** and humidity up to **90 percent non-condensing**.

16. Lifecycle requirements shall include:

a. minimum **five (5) years OEM support** for security updates and spare parts;
b. minimum **three (3) years comprehensive warranty**;
c. availability of remote diagnostics and automated fault reporting; and
d. documented end-of-life management and disposal through approved handlers.

**Compliance with Procurement and Clearance Requirements**

17. All network-related procurements shall comply with:
a. the minimum technical baseline requirements in this Part;
b. applicable tier-based requirements in **Annex C**;
c. NITDA IT Project Clearance requirements; and
d. applicable public procurement regulations.

18. Only vendors and equipment validated as compliant with this Guideline shall be approved for deployment within government networks.

**Network Architecture Baseline**

19. The minimum technical requirements defined in this Part apply to **individual network components and systems** deployed within Federal Public Institutions.
20. In addition to equipment capabilities, institutions shall ensure that network infrastructure is deployed within **secure and resilient network architectures** that support operational continuity and cybersecurity.
21. Such architecture shall include appropriate implementation of:

a. network segmentation;
b. management network isolation;
c. security zones for public-facing services; and
d. redundancy and failover mechanisms.

22. The **minimum architecture and resilience controls necessary to support these objectives are specified in Annex D of this Guideline**.
23. Compliance with Annex D shall form part of the network infrastructure audit conducted under **Part III of this Guideline**.

## PART V – AUDIT OUTPUTS, REPORTING, AND DOCUMENTATION

### Audit Outputs

1. Each audit conducted under this Guideline shall produce the following mandatory outputs:
   a. a **completed Network Audit Checklist** in the format set out in **Annex A**;
   b. a **validated network asset register** covering all assets assessed; and
   c. a **compliance summary** indicating compliance status by asset category and overall institutional status.
2. Audit outputs shall reflect results recorded using **binary (Yes/No)** or **quantitative measurements** only.

### Audit Reporting Requirements

3. An audit conducted under this Guideline shall result in a **Network Audit Report** containing, at a minimum:
   a. the name of the institution audited;
   b. the applicable **tier classification** under Part II;
   c. the scope and date of the audit;
   d. a summary of audit results by asset category;
   e. the overall compliance status determined in accordance with **Annex B**; and
   f. an index of supporting evidence.

4. Audit reports shall not include subjective opinions, narrative scoring, or maturity assessments beyond what is required to record objective findings.

### Documentation and Evidence Management

5. Federal Public Institutions shall maintain documentation supporting audit results, including:
   a. completed audit checklists;
   b. asset registers;
   c. configuration records and system outputs;
   d. OEM documentation and warranty records; and
   e. monitoring logs and retention records.

6. Documentation shall be:

   a. accurate and complete;
   b. traceable to specific network assets; and
   c. protected against unauthorised alteration or deletion.

### Record Retention

7. Audit reports, checklists, and supporting documentation shall be retained in accordance with applicable government record-management requirements.

8. Where no specific retention period applies, audit records shall be retained for a minimum period sufficient to support:

   a. regulatory review;
   b. compliance verification; and
   c. validation of future procurements under the **NITDA IT Project Clearance** process.

### Use of Audit Outputs

9. Audit outputs generated under this Part may be used to:
   a. establish baseline compliance status of network infrastructure;
   b. inform remediation planning and prioritisation;
   c. support decision-making for upgrades or replacements; and
   d. validate alignment of proposed network procurements with this Guideline.

10. Audit outputs shall not replace or override statutory approval processes but shall serve as **technical evidence** for regulatory and clearance purposes.

### Consistency and Traceability

11. Audit outputs and reports shall reference the **version of this Guideline** applicable at the time of audit.

12. Where audits are conducted across different cycles or guideline revisions, the aplicable version shall be clearly indicated to preserve traceability and consistency.

## PART VI – COMPLIANCE, BREACH, AND SANCTIONS

### Compliance Determination

1. Compliance with this Guideline shall be determined based on:
   a. audit results recorded in accordance with **Part III**; and
   b. compliance scoring conducted in accordance with **Annex B**.

2. An institution shall be classified as:

   a. **Compliant**;

b. **Partially Compliant**; or

c. **Non-Compliant**, based strictly on objective audit outcomes and recorded evidence.

3. Compliance determination shall not be subject to discretionary adjustment outside the parameters defined in this Guideline.

### Breach of the Guideline

4. A breach of this Guideline occurs where a Federal Public Institution:
   a. fails to meet one or more mandatory minimum technical baseline requirements under **Part IV**;
   b. fails to meet applicable tier-based minimum requirements specified in **Annex C and D**;
   c. deploys network infrastructure procured without compliance with **NITDA IT Project Clearance**; or
   d. provides false, misleading, incomplete, or unsupported information during an audit.

5. A breach may arise from acts of omission or commission, including failure to remediate identified non-compliance within a reasonable timeframe.

### Sanctions

6. Where a breach is established, NITDA may impose one or more of the following sanctions, proportionate to the nature and severity of the breach:
   a. issuance of a **compliance directive** requiring remediation within a specified timeframe;
   b. classification of the institution as **Non-Compliant** for regulatory and clearance purposes;
   c. suspension or withholding of approval under the **IT Project Clearance** process for affected network procurements;
   d. mandatory re-audit following remediation; or
   e. any other non-monetary regulatory measure within NITDA’s statutory powers.

7. Sanctions under this Guideline are **administrative and corrective in nature** and shall not preclude the application of other lawful measures under applicable laws.

### Procedure for Administration of Sanctions

8. Before imposing any sanction, NITDA shall:
   a. notify the affected institution in writing of the identified breach;

b. specify the provisions breached and the supporting audit evidence; and
c. provide a reasonable opportunity for the institution to respond or remedy the breach.

9. In determining appropriate sanctions, NITDA shall consider:

   a. the criticality of the affected systems;
   b. the tier classification of the institution;
   c. the risk posed to government operations or public service delivery; and
   d. whether the breach is recurrent or systemic.

10. Decisions on sanctions shall be documented and communicated formally to the affected institution.

### Effect of Non-Compliance

11. An institution classified as **Non-Compliant** may be subject to enhanced oversight and prioritised remediation requirements.

12. Persistent non-compliance may be taken into account during future IT Project Clearance reviews and regulatory engagements.

## PART VII – MISCELLANEOUS PROVISIONS

### Review and Amendments

1. NITDA may, from time to time, **review, revise, or amend** this Guideline to reflect:

   a. changes in technology or emerging risks;
   b. developments in government digital service delivery;
   c. lessons learned from audits and implementation; or
   d. alignment with updated national policies or laws.

2. Any review or amendment under this Section shall be carried out in consultation with relevant stakeholders, where appropriate.

3. Amendments to this Guideline shall take effect on the date specified by NITDA and shall not invalidate audits or compliance determinations made prior to such amendments.

### Dispute Resolution Mechanism

4. Any dispute arising from the interpretation or application of this Guideline shall, in the first instance, be resolved through **administrative engagement** with NITDA.

5. Where a dispute is not resolved through administrative engagement, the affected institution may escalate the matter in accordance with applicable government dispute resolution or review mechanisms.

6. Nothing in this Section shall prejudice the right of any party to seek redress under applicable laws.

**Transitional Provisions**

7. Federal Public Institutions shall be afforded a **reasonable transitional period**, as may be determined by NITDA, to address non-compliance identified during initial audits conducted under this Guideline.

8. Transitional arrangements shall not apply to:

   a. new network procurements subject to IT Project Clearance; or
   b. deployments that pose immediate or material risk to government operations or public service delivery.

**Savings**

9. Nothing in this Guideline shall be construed as invalidating:
   a. audits conducted prior to its commencement; or
   b. approvals lawfully granted before the coming into force of this Guideline.

10. Existing approvals and actions shall continue to have effect until reviewed or superseded in accordance with this Guideline.

## Part VIII – Structure and Use of the Annexes

### Purpose of the Annexes

1. The Annexes to this Guideline provide the **operational instruments required for the practical implementation of the Government Network Infrastructure Baseline and Audit Guideline (GNIA)**.

2. While the main body of the Guideline establishes the **legal basis, governance framework, and minimum technical baseline requirements**, the Annexes provide:

a. structured tools for conducting network infrastructure audits;
b. a standardised method for determining compliance status;
c. tier-conditioned enhancements applicable to institutions of different operational scale and risk exposure; and
d. supporting controls that ensure network resilience and architectural integrity.

3. The Annexes therefore serve as the **technical implementation layer of the Guideline** and shall be applied together with the provisions of Parts II, III, and IV.

**Legal Status of the Annexes**

1. The Annexes form an **integral part of this Guideline** and shall have the same regulatory force as the provisions contained in the main body of the document.
2. Compliance with the provisions contained in the Annexes shall therefore be **mandatory wherever referenced in the relevant Parts of this Guideline**.
3. Where a requirement in the Annexes clarifies or operationalises a provision in the main text, the Annex shall be interpreted as **supplementary and explanatory rather than substitutive**.
4. In the event of ambiguity between the narrative provisions of this Guideline and the operational mechanisms defined in the Annexes, the interpretation that **best preserves audit objectivity and baseline technical compliance shall prevail**.

## Abbreviations

For the purposes of this Guideline, the following abbreviations shall apply:

- **AES** – Advanced Encryption Standard
- **BPP** – Bureau of Public Procurement
- **FPI** – Federal Public Institution
- **GNIA** – Government Network Infrastructure Baseline and Audit Guideline
- **IP** – Internet Protocol
- **IT** – Information Technology
- **NITDA** – National Information Technology Development Agency
- **OEM** – Original Equipment Manufacturer
- **QoS** – Quality of Service
- **SIEM** – Security Information and Event Management

**Overview of the Annex Structure**

This Guideline contains four Annexes, each performing a distinct function within the GNIA framework:

| **Annex** | **Title** | **Primary Function** |
|---|---|---|
| Annex A | Network Audit Checklist | Provides the standardised instrument for auditing network infrastructure assets |
| Annex B | Baseline Compliance Scoring Matrix | Defines the scoring model used to determine compliance status |
| Annex C | Tier-Based Minimum Network Infrastructure Requirements | Establishes additional minimum requirements applicable to higher-tier institutions |
| Annex D | Minimal Network Architecture and Resilience Controls | Defines structural network controls necessary to ensure segmentation, redundancy, and resilience |

These Annexes operate together to provide a **complete and self-executing compliance system**.

**Annex A – Network Audit Checklist**

1. Annex A provides the **standardised checklist used to assess network infrastructure assets** during audits conducted under Part III of this Guideline.
2. The checklist translates the minimum technical baseline requirements defined in Part IV into **objective audit parameters**.
3. Each checklist entry records:

   a. the infrastructure component assessed;
   b. the minimum requirement applicable;
   c. the audit result expressed as a binary or quantitative value; and
   d. the reference to supporting evidence.

4. The checklist is designed to ensure that audits conducted under this Guideline are:

   a. repeatable;
   b. evidence-based; and
   c. free from subjective interpretation.

5. Federal Public Institutions may also use Annex A as a **self-assessment tool** prior to formal audit exercises.

### Annex B – Baseline Compliance Scoring Matrix

1. Annex B establishes the **standardised scoring methodology** used to convert audit results recorded in Annex A into an overall compliance score.
2. The scoring matrix provides:

   a. the scoring rules applied to individual audit items;
   b. the weighting assigned to each technical category;
   c. the calculation method used to determine overall compliance scores; and
   d. the thresholds used to classify institutions as Compliant, Partially Compliant, or Non-Compliant.

3. Annex B also defines **critical-failure override conditions**, which ensure that certain foundational security failures cannot be masked by otherwise acceptable aggregate scores.
4. The scoring matrix therefore ensures that compliance determination remains **objective, transparent, and consistent across all Federal Public Institutions**.

### Annex C – Tier-Based Minimum Network Infrastructure Requirements

1. Annex C establishes **additional mandatory minimum requirements** applicable to institutions based on their Tier Classification under Part II.
2. These requirements reflect the principle that institutions operating **higher-risk, high-availability, or nationally critical digital services require stronger infrastructure controls**.
3. Annex C therefore introduces tier-conditioned enhancements in areas including:

   a. core infrastructure resilience;
   b. network security and high availability;
   c. monitoring and operational visibility; and
   d. switching and wireless network capabilities.

4. The tier framework ensures that the GNIA remains **risk-aware and proportionate**, while preserving a single national baseline applicable to all institutions.

5. Tier-based requirements shall **supplement but never replace** the baseline requirements defined in Part IV.

### Annex D – Minimal Network Architecture and Resilience Controls

1. Annex D establishes minimum architectural controls required to ensure that government networks are **securely segmented, resilient to failure, and capable of supporting mission-critical digital services**.
2. The controls in Annex D focus on **structural characteristics of network infrastructure**, including:

   a. logical network segmentation;
   b. separation of management and operational networks;
   c. implementation of security zones such as DMZ and guest networks; and
   d. redundancy and failover mechanisms.
3. These controls ensure that compliant network equipment is deployed within **secure and resilient architectural environments**, thereby reducing systemic vulnerabilities.
4. Annex D is intentionally limited to **minimum architecture controls necessary to support auditability and resilience** and does not prescribe detailed network design models.

### Integrated Use of the Annexes

1. The Annexes are intended to be used **together as a single compliance mechanism**, as illustrated below:

   Step 1 – Tier Identification
   The institution is classified using the Tier Classification Framework in Part II.

   Step 2 – Infrastructure Audit
   Network assets are assessed using the Network Audit Checklist in Annex A.

   Step 3 – Tier-Based Requirement Validation
   Additional requirements applicable to the institution’s tier are verified using Annex C.

   Step 4 – Architecture Control Verification
   Structural network resilience and segmentation controls are assessed using Annex D.

Step 5 – Compliance Scoring
Audit results are converted into a compliance score using the Baseline Compliance Scoring Matrix in Annex B.

2. This integrated approach ensures that the Guideline can be implemented **without the need for additional operational procedures or interpretation frameworks**.

**Review and Evolution of Annexes**

1. NITDA may review and update the Annexes to reflect:

   a. technological advancements;
   b. evolving cybersecurity threats;
   c. lessons learned from audit exercises; or
   d. changes in national digital infrastructure priorities.

2. Updates to the Annexes shall not invalidate audits conducted under earlier versions of this Guideline, provided that the applicable version is clearly documented.

## ANNEX A – NETWORK AUDIT CHECKLIST

*(Issued pursuant to Part III of the Government Network Infrastructure Baseline and Audit Guideline)*

### A1. Institution and Audit Details

| Item | Information |
|---|---|
| Federal Public Institution | |
| Tier Classification | Tier 1 / Tier 2 / Tier 3 |
| Audit Scope | |
| Audit Date | |
| Audit Reference | |
| Auditor | |
| Guideline Version | |

### A2. Core Network Infrastructure (Core Routers)

| Requirement | Minimum Requirement | Result | Evidence |
|---|---|---|---|
| Forwarding Capacity | ≥10 Gbps | | |
| IPv6 Support | Enabled | | |
| Routing Protocols | OSPF, BGP | | |
| Redundant Power Supplies | Dual | | |
| Redundant Route Processors | Enabled | | |
| Hardware Encryption | AES-256+ | | |
| Secure Boot | Enabled | | |
| Role-Based Access Control | Enabled | | |
| QoS / Policy Routing | Enabled | | |
| Availability Design | ≥99.99% | | |

### A3. Edge Routing and Security (NGFW)

| Requirement | Minimum | Result | Evidence |
|---|---|---|---|
| Inspection Capacity | ≥2.5 Gbps | | |
| Deep Packet Inspection | Enabled | | |
| IPS / IDS | Enabled | | |
| Application Control | Enabled | | |
| Anti-Malware / Web Filtering | Enabled | | |
| IPsec / SSL VPN | Enabled | | |
| Encryption Throughput | ≥1 Gbps | | |
| High Availability | Active-Passive / Active-Active | | |
| Failover Time | ≤5 seconds | | |
| Syslog Export | Enabled | | |
| NetFlow/IPFIX | Enabled | | |
| SIEM Integration | Tier-based | | |

### A4. Switching Infrastructure

| Requirement | Minimum | Result | Evidence |
|---|---|---|---|
| Access Switching | Layer 2 Gigabit | | |
| Distribution/Core Switching | Layer 3 ≥10 Gbps | | |
| Port Density | ≥24 Ports | | |
| PoE Support | IEEE 802.3af/at/bt | | |
| VLAN Support | Enabled | | |
| QoS | Enabled | | |
| LACP | Enabled | | |
| Spanning Tree | Enabled | | |
| DHCP Snooping | Enabled | | |

| | | | |
|---|---|---|---|
| 802.1X NAC | Tier-based | | |
| Secure SSH Access | Enabled | | |
| SNMPv3 | Enabled | | |
| Configuration Backup | Enabled | | |

### A5. Wireless Infrastructure

| Requirement | Minimum | Result | Evidence |
|---|---|---|---|
| Wireless Standard | Wi-Fi 6 | | |
| Frequency Bands | 2.4 GHz / 5 GHz | | |
| Concurrent Clients | ≥50 per AP | | |
| Throughput | ≥1.5 Gbps | | |
| Encryption | WPA3 | | |
| VLAN Segmentation | Enabled | | |
| RADIUS / 802.1X | Enabled | | |
| Wireless Controller | Tier-based | | |
| RF Optimisation | Tier-based | | |
| Enclosure | ≥IP54 | | |

### A6. Network Monitoring and Visibility

| Requirement | Minimum | Result | Evidence |
|---|---|---|---|
| Monitoring Dashboard | Available | | |
| SNMPv3 | Enabled | | |
| Syslog | Enabled | | |
| NetFlow/IPFIX | Enabled | | |
| Threshold Alerts | Enabled | | |
| Predictive Capacity Monitoring | Tier-based | | |
| Log Retention | ≥12 months | | |

| | | | |
|---|---|---|---|
| National/NITDA NOC Integration | Tier-based | | |
| 24/7 Monitoring | Tier-based | | |

### A7. Energy Efficiency & Lifecycle

| Requirement | Minimum | Result | Evidence |
|---|---|---|---|
| Energy Certification | Energy Star / Equivalent | | |
| Operating Temperature | 0–45°C | | |
| OEM Support | ≥5 years | | |
| Warranty | ≥3 years | | |
| Security Patch Status | Current | | |
| Diagnostics | Remote | | |
| Fault Reporting | Automated | | |
| End-of-Life Status | Not EoL | | |

### A8. Architecture and Resilience Controls (See Annex D)

| Requirement | Result | Evidence |
|---|---|---|
| Network Segmentation Implemented | | |
| Minimum Zones by Tier | | |
| DMZ for Public Services | | |
| Guest Network Isolation | | |
| Management Network Separation | | |
| Firewall High Availability | | |
| Core Redundancy | | |
| Internet Failover | | |
| Architecture Documentation | | |

## ANNEX B – BASELINE COMPLIANCE SCORING MATRIX

### B1 Purpose

This Annex defines the scoring mechanism used to convert audit results into compliance status.

### B2 Scoring Rules

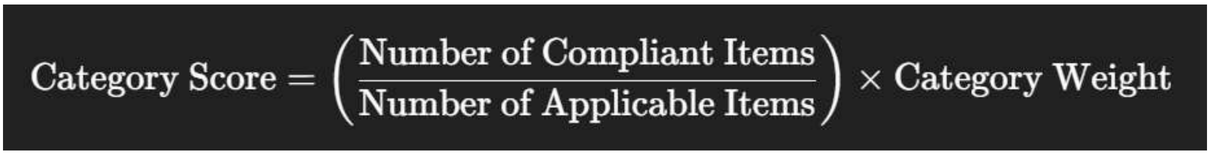
| Result | Score |
|---|---|
| Compliant | 1 |
| Non-Compliant | 0 |

Not Applicable items are excluded.

### B3 Category Weighting

| Category | Weight |
|---|---|
| Core Infrastructure | 25% |
| Edge Security | 25% |
| Switching | 15% |
| Wireless | 10% |
| Monitoring | 10% |
| Energy/Lifecycle | 10% |
| Architecture Controls | 5% |
| Total | 100% |

### B4 Compliance Thresholds: For each category:



$$\text{Category Score} = \left(\frac{\text{Number of Compliant Items}}{\text{Number of Applicable Items}}\right) \times \text{Category Weight}$$

| Score | Status |
|---|---|
| 90-100% | Compliant |
| 70-89% | Partially Compliant |
| <70% | Non-Compliant |

## B5. Audit Outcome Summary

| **Category** | **Status (Compliant, Partially Compliant or Non-Compliant)** |
|---|---|
| Core Infrastructure | |
| Edge & Security | |
| Switching | |
| Wireless | |
| Monitoring | |
| Lifecycle | |
| Architecture | |
| Overall Compliance | |

## B6 Critical Failure Override

Non-compliance occurs automatically if any of the following fail:

1. Core router redundancy
2. Firewall IPS/DPI capability
3. Secure boot firmware
4. Centralised logging
5. OEM support status

## ANNEX C – TIER-BASED MINIMUM NETWORK REQUIREMENTS

*(Aligned to Part II and Part IV)*

### C1 Purpose

Defines enhanced requirements for higher-criticality institutions.

### C2 Core Infrastructure

| Requirement | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| Throughput | ≥10 Gbps | ≥10 Gbps | ≥10 Gbps |
| Modular Scalability | Optional | Mandatory | Mandatory |
| Redundant Route Processors | Optional | Mandatory | Mandatory |
| Availability | ≥99.9% | ≥99.99% | ≥99.99% |

### C3 Security

| Requirement | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| IPS/DPI | Mandatory | Mandatory | Mandatory |
| Firewall HA | Optional | Mandatory | Mandatory |
| Failover | ≤10 sec | ≤5 sec | ≤5 sec |

### C4 Monitoring

| Requirement | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| Monitoring Dashboard | Mandatory | Mandatory | Mandatory |
| Log Retention | ≥6 months | ≥12 months | ≥12 months |
| 24/7 Monitoring | No | Optional | Mandatory |
| National NOC Integration | Optional | Mandatory | Mandatory |

## ANNEX D – MINIMAL NETWORK ARCHITECTURE AND RESILIENCE CONTROLS

### D1 Purpose

Defines minimal architecture controls necessary to ensure network resilience and segmentation.

### D2 Minimum Segmentation

| Tier | Minimum Zones |
|---|---|
| Tier 1 | 3 (where applicable) |
| Tier 2 | 5 |
| Tier 3 | 5+ |

Required zones:

1. User Network
2. Server/Data Network
3. Management Network
4. DMZ
5. Guest Network

### D3 Management Network

Administrative access must occur via:

1. dedicated management VLAN
2. role-based access control
3. secure authentication

### D4 Network Redundancy

| Control | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| Core Redundancy | Optional | Mandatory | Mandatory |
| Firewall HA | Optional | Mandatory | Mandatory |
| Dual Uplinks | Optional | Mandatory | Mandatory |
| Internet Failover | Optional | Mandatory | Mandatory |

### D5 Documentation

Institutions must maintain:

1. network topology diagrams
2. VLAN/subnet allocation
3. firewall policy summaries
4. network asset inventory