

SEPTEMBER 5, 2025



SUDESA MISSION PLAN

FOR A DIGITALIZED, INCLUSIVE AND WELL-DEVELOPED SOUTH SUDAN

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Executive Summary	6
Mission Statement.....	7
Legal Basis, Scope, and Definitions	7
Document Control and Versioning	8
1. Strategic Rationale and Theory of Change.....	8
1.1 Context and Problem Statement.....	8
1.2 Strategic Rationale for Digitalisation	9
1.3 Theory of Change and Impact Pathway	9
2. Mission Objectives and Success Criteria	11
2.1 Strategic Objectives	11
2.2 Operational Objectives	12
2.3 Key Performance Indicators and Targets (Multi-Tier Results Framework)	13
2.4 Success Criteria and Conditions for Sustainability.....	15
2.5 Alignment with Global and Regional Frameworks	16
2.6 Calculation Notes and Verification	16
3. Implementation Strategy and Phasing (10-Year Programme)	17
3.1 Programme Architecture and Decision Rights	17
3.2 Phasing Overview (Years 1–10)	17
3.3 The First 90 Days and Year 1 Milestones.....	18
3.4 Stage-Gates and Decision Thresholds	18
3.5 Workstream Roadmaps	19
3.6 Resourcing and Capacity Transfer	19
3.7 Financing, Disbursement, and Cost Recovery.....	20
3.8 Procurement Strategy and Vendor Neutrality	20
3.9 Risk Management and Contingencies	20
3.10 Ten-Year Timeline.....	20
3.11 Exit, Handover, and Sustainability.....	20
4. Institutional Architecture and Decision Rights	21
4.1 SUDESA Secretariat and Core Departments.....	21
4.2 Digital Transformation Steering Committee (DTSC)	22
4.3 Joint Steering Committee (JSC).....	23
4.4 Delegations of Authority and Escalation Protocols	24
5. Digital Government Blueprint (Microsoft Government Solutions)	25
5.1 Enterprise Architecture and Interoperability.....	25



5.2 Identity, Access, and Digital ID	25
5.3 Microsoft 365 Deployment (Collaboration, Compliance, and Operations)	26
5.4 Azure Hosting with Sovereign Controls (Hybrid Pattern)	26
5.5 Zero-Trust Security Architecture and SOC Operations	27
5.6 Digital Public Services and Citizen Portals (Service Design, Back-Office, and Assurance)	27
Compliance Mapping (Indicative)	29
6. Education Digitalisation Programme (Universities, TVET, Primary and Secondary)	29
6.1 Pedagogical Intent and System Design Principles	29
6.2 Universities and TVET (with Applied Digital & Fibre Tracks)	29
6.3 Primary and Secondary Education (Sequenced Rollout)	30
6.4 Devices, Device Management, and Labs	30
6.5 School Connectivity and Community Benefit	30
6.6 Safety, Privacy, and Data Governance in Education	31
6.7 Platforms, Content, and Assessment	31
6.8 Monitoring, Evaluation, and Learning (MEL)	31
7. Open-Access Community Broadband (Swedish Model Inspired)	31
7.1 Policy Model and Rationale	31
7.2 Building-Level Fibre and the Neutral-Host Network	32
7.3 Wholesale Access, ISP Marketplace, and Competition	32
7.4 Rights-of-Way, Building Codes, and Wayleave Framework	33
7.5 Universal Service, Affordability, and Last-Mile Options	33
7.6 Satellite and Resilience for Remote Areas	33
Pricing, Subsidy, and Thresholds: How the Affordability Period Works	34
Governance, Transparency, and Investor Protections	34
Outcome: A Neutral, Publicly Owned Spine with Vibrant Private Competition	34
8. Compliance, Data Protection, and Cybersecurity	34
8.1 Data Protection and Privacy Framework (DPIA Regime)	35
8.2 Cybersecurity Framework (ISO/IEC 27001:2022; NIST CSF 2.0)	35
8.3 Government CERT and Incident Response	36
8.4 Information Governance, Records, and Audit Trails	38
9. Procurement, Open Contracting, and Vendor Neutrality	39
9.1 Procurement Policy and Procedures	39
9.2 Open Contracting Data Standard (OCDS) Publication	40
9.3 Competition, Beneficial Ownership, and Complaints Handling	41
9.4 Anti-Lock-In Measures and Open Standards	42



10. Financing Architecture and Fiduciary Controls	43
10.1 Digital Transformation Investment Facility (DTIF)	43
10.2 IPSAS-Compliant Financial Management.....	44
10.3 Disbursement, Treasury, and Cost Recovery Policy	44
10.4 Partner Contributions and Co-Financing Modalities	45
11. ESG Safeguards and Human Rights	45
11.1 Environmental and Social Frameworks (WB ESF; AfDB ISS)	45
11.2 SEA/SH Prevention and Response	46
11.3 Community Health, Safety, and Grievance Redress	46
11.4 E-Waste, Energy, and Green Data Centres	47
12. Monitoring, Evaluation, and Learning (MEL)	47
13. Risk Management and Contingency Planning	49
13.1 Strategic, Operational, and Fiduciary Risks.....	49
13.2 Cyber, Data, and Continuity Risks	50
13.3 Mitigation Measures and Contingency Reserves.....	50
13.4 Risk Register Governance	51
14. Stakeholder Engagement and Communications.....	52
14.1 Government, Parliament, and Sub-National Interfaces	52
14.2 Development Partners and Private Sector.....	52
14.3 Civil Society, Traditional and Faith Leaders, and Diaspora	52
14.4 Public Communications, Branding, and Disclosure	52
15. Alignment with Various Agendas	53
15.1 Alignment with the United Nations Sustainable Development Goals (SDGs).....	53
15.2 Alignment with the African Union Agenda 2063	53
15.3 Alignment with the Social Global Goals (SGGs) under Agenda for Social Equity 2074	53
15.4 Financing and Compliance Anchoring under Agenda 2074.....	54
1. Global and Continental Agendas	54
2. Digital Transformation and Procurement Standards	54
3. Fiduciary and Financial Management	55
4. ESG and Safeguards	55
5. Cybersecurity and Data Governance.....	55
6. Monitoring, Evaluation, and Learning (MEL)	55
7. Dispute Resolution and Arbitration	55
16. SWOT Analysis (Digital, Education, and Broadband).....	56
16.1 Strengths and Weaknesses.....	56



16.2 Opportunities and Threats	56
SWOT Table	57
17. PESTEL Analysis	57
17.1 Political and Economic	57
17.2 Social and Technological	58
17.3 Environmental and Legal	58
PESTEL Analysis Table – South Sudan (Digitalisation, Education, and Broadband)	59
18. Legal and Policy Roadmap	59
18.1 Data Protection & Privacy Act	59
18.2 Digital Identity Act	60
18.3 Cybersecurity Law and CERT Designation	60
18.4 E-Procurement and Open Contracting Reforms	60
18.5 Broadband and Spectrum Policy; Building Regulations	60
Institutional Anchoring and Compliance	61
19. Capacity Building and Change Management	61
19.1 Civil Service Digital Competencies	61
19.2 Institutional Reform and Job Profiles	61
19.3 Local Vendor Ecosystem and Certification	61
19.4 Leadership, Incentives, and Change Champions	62
20. Sustainability and Exit Strategy	62
20.1 Operations and Maintenance (O&M) and Lifecycle Financing	62
20.2 Institutionalisation within National Systems	62
20.3 Handover, Local Ownership, and Cost Recovery	63
20.4 Long-Term Governance and Strategic Adaptation	63
Annex A: Acronyms and Glossary	64
Annex E: Technical Annex – Enterprise Architecture and Standards	65
Annex F (Legal Draft): Open Access Broadband — Technical and Regulatory Notes	67
Annex H: Risk Register Template and Guidance	79
Annex I: Communications and Disclosure Protocols	85
Annex J: Device Specification and Lifecycle Policy	89
Annex K: Accessibility and Inclusion Standards (Education)	91

SUDESA Mission Plan

Executive Summary

The Republic of South Sudan stands at a pivotal juncture in its nation-building journey. The absence of a unified digital infrastructure, coupled with fragmented governance systems and limited connectivity, has constrained service delivery, economic participation, and social inclusion. This Mission Plan responds to these structural challenges with a transformative agenda: to establish a digitally sovereign, inclusive, and future-ready South Sudan through the South Sudan Development and Social Equity Agency (SUDESA).

Purpose and Strategic Intent

The Mission seeks to modernise governance, empower citizens, and catalyse economic growth by embedding digitalisation as a foundational pillar of state-building. It is not a technology project; it is a social contract anchored in the principles of sovereignty, equity, and sustainability. By leveraging secure, enterprise-grade solutions and open-access infrastructure models, the Mission aims to create a resilient digital ecosystem that serves the people—not the system—and endures beyond political cycles.

Core Pillars of Transformation

1. Digital Government Enablement

The first priority is to replace insecure, consumer-grade platforms with a sovereign, interoperable, and secure digital backbone for government operations. This will be achieved through the deployment of Microsoft Government solutions, including Microsoft 365 Government Suite and Azure Government Cloud, under a Zero-Trust security architecture. These systems will enable e-Government services, digital identity, and data-driven governance.

2. Education Digitalisation

Education is the catalyst for long-term social equity. The Mission adopts a phased approach:

- **Short Term:** Digitalise universities and vocational institutions to strengthen higher education and workforce readiness.
- **Long Term:** Extend digitalisation to primary and secondary schools, ensuring that every child grows up with access to digital tools and learning resources. This approach addresses both immediate capacity gaps and intergenerational equity.

3. Open Access Broadband Infrastructure

Inspired by the Swedish community broadband model, the Mission will implement an open-access fiber network at the building and community level. This neutral-host model allows multiple Internet Service Providers (ISPs) to compete on service quality and price, ensuring affordability, universal access, and local economic empowerment. Satellite and wireless solutions will complement fiber in remote areas, guaranteeing nationwide coverage.

Alignment and Compliance

The Mission is fully aligned with the Agenda for Social Equity 2074, the African Union's Agenda 2063, and the UN Sustainable Development Goals (SDGs). It embeds global best practices in data protection, cybersecurity (ISO/IEC 27001; NIST CSF 2.0), and fiduciary governance (IPSAS standards), ensuring

eligibility for concessional finance from development partners such as the African Development Bank, Nordic DFIs, and the World Bank.

Financing and Governance

The Digital Transformation Investment Facility (DTIF) will serve as the pooled financing mechanism for this Mission, operating under a robust fiduciary framework with independent audits, open contracting standards, and ESG safeguards. Governance will be exercised through the Joint Steering Committee and the Digital Transformation Steering Committee, ensuring transparency, accountability, and policy continuity.

Impact and Legacy

This Mission is designed to deliver measurable outcomes: improved governance efficiency, enhanced education access, expanded connectivity, and inclusive economic growth. It positions South Sudan as a regional leader in ethical digital transformation and sets a precedent for fragile states globally. Above all, it ensures that technology becomes a tool for equity, dignity, and progress—anchored in the values of Agenda 2074 and owned by the people of South Sudan.

Mission Statement

“To establish a digitally sovereign, inclusive, and future-ready South Sudan by modernising governance systems, enabling universal access to education, and creating an open, competitive broadband ecosystem. Through SUDESA, this Mission integrates secure digital infrastructure, public sector reform, and human capital development under Agenda for Social Equity 2074—ensuring that technology serves the people, strengthens sovereignty, and drives sustainable development for generations to come.”

Legal Basis, Scope, and Definitions

This Mission Plan is issued pursuant to:

- The **Strategic Engagement Agreement** between the Government of the Republic of South Sudan and the European Social Label (EUSL).
- The **Host Country Agreement** establishing SUDESA as a semi-autonomous, co-owned institutional entity with legal personality, administrative autonomy, and operational capacity.
- The **Charter and Operating Manual of the Digital Transformation Investment Facility (DTIF)**, which governs fiduciary management, procurement, and safeguards for all digitalisation-related investments.
- The **Institutional Framework and Governance Manual for SUDESA**, which defines governance bodies, decision-making protocols, and compliance obligations.

Scope:

This Mission Plan applies to all programmes, projects, and activities executed under SUDESA’s mandate in the domains of digital transformation, education digitalisation, and broadband infrastructure development. It is binding upon all implementing entities, contractors, and partners engaged under the DTIF framework.

Definitions:

- **“Agenda 2074”** refers to the Agenda for Social Equity 2074, a long-term strategic framework for inclusive development and governance.



- **“Microsoft Government Solutions”** refers to the suite of enterprise-grade digital tools, including Microsoft 365 Government and Azure Government Cloud, deployed for public sector operations.
- **“Open Access Broadband Model”** refers to a neutral-host infrastructure framework enabling multiple ISPs to provide services over shared fiber networks, ensuring affordability and competition.
- **“DTIF”** refers to the Digital Transformation Investment Facility, the pooled financing mechanism for digitalisation initiatives under SUDESA.

Document Control and Versioning

- **Document Title:** SUDESA Mission Plan
- **Version:** 1.0 (Draft for Presidential and Ministerial Review)
- **Date of Issue:** [Insert Date]
- **Prepared by:** European Social Label (EUSL) in collaboration with the Government of the Republic of South Sudan
- **Approved by:** [To be completed upon adoption]
- **Distribution:** Office of the President, Ministry of ICT, Ministry of Finance and Planning, Ministry of General Education and Instruction, Development Partners, and SUDESA Governance Bodies.

1. Strategic Rationale and Theory of Change

1.1 Context and Problem Statement

South Sudan’s public administration, education system, and connectivity landscape exhibit structural constraints that impede effective service delivery, citizen participation, and inclusive growth. Internet use remains among the lowest globally: independent compilations estimated roughly **7% internet penetration** in early 2023, reflecting a narrow base of connected users relative to population, while broader ITU/WB trend series underscore persistent gaps in access, affordability, and rural coverage typical of least-connected markets.

The state’s transition toward resilient digital institutions is further challenged by the absence of a sovereign, interoperable, and secure backbone for government operations, together with limited last-mile broadband and fragmented data governance arrangements—risks well-documented across fragile and low-income contexts by global GovTech diagnostics and digital infrastructure briefs.

In education, digital exclusion reinforces inequality. UNESCO finds that digital technologies—when embedded in sound policy and teacher support—can **complement, enrich, and transform** teaching and administration, yet significant gaps in device access, connectivity, and digital competences persist across Sub-Saharan systems.

Rigorous evidence reviews of EdTech in developing countries further show that **instruction-enhancing and self-led learning** solutions are those most consistently associated with learning gains, whereas mere hardware access is insufficient without aligned pedagogy and support.

From a legal and institutional perspective, South Sudan must converge toward continental norms. The African Union’s **Digital Transformation Strategy for Africa (2020–2030)** calls for secure, affordable

broadband, harmonized data frameworks, and the scaling of digital public services; the **Malabo Convention** sets a treaty-level baseline for cybersecurity and personal-data protection to underpin trusted digital economies.

Donor eligibility and risk management likewise require risk-based safeguards consistent with the World Bank's **Environmental and Social Framework (ESF)** and the African Development Bank's **updated Integrated Safeguards System (ISS)**, effective **31 May 2024**.

1.2 Strategic Rationale for Digitalisation

The Mission adopts a state-building logic: a **sovereign, secure, and interoperable digital backbone** is a prerequisite for credible public services, fiscal efficiency, and citizen trust. The deployment of a **Zero-Trust** cybersecurity architecture aligned to the **NIST Cybersecurity Framework 2.0** and the **ISO/IEC 27001:2022** information-security management standard addresses contemporary threat surfaces while enabling proportionate, auditable controls across ministries and tiers of government.

The same controls are necessary to protect learners and institutions as education is digitalised, and to safeguard the integrity of national identity, registries, and payments platforms. The World Bank's **ID4D Principles** reinforce technology neutrality, privacy-by-design, and inclusion, guiding the design of digital identity and registries consistent with rights and accountability.

To ensure fiduciary integrity and market confidence, the Mission mainstreams **open contracting**: structured disclosure of the full contracting cycle using the **Open Contracting Data Standard (OCDS)** improves value-for-money analytics, expands competition, and equips oversight bodies and the public to detect red flags.

This approach complements the ESF/ISS safeguards, creating an integrated assurance stack spanning procurement transparency, environmental and social risk management, and auditability.

On connectivity, the Mission proposes an **open-access, neutral-host broadband** model—adapting Sweden's municipal and community **open network** practice (e.g., Stockholm's **Stokab** dark-fibre utility and the three-layer owner–operator–service-provider model). Such models have demonstrably **increased FTTP coverage, enabled retail competition, and lowered barriers to entry** by separating passive infrastructure from active services and retail provision.

This design is suited to attract multiple ISPs, align with community broadband in multi-dwelling units and cooperatives, and can be complemented with satellite and fixed-wireless for hard-to-reach areas. It is also consistent with Sweden's national connectivity strategy that emphasizes ubiquitous, high-quality access through coordinated public–private deployment and mapping.

In education, a phased pathway—**universities and TVET first**, followed by **primary and secondary**—is justified by the evidence and capacity realities: higher-education digitalisation can quickly strengthen the pipeline of teachers, health professionals, and civil servants, while the long-term equity dividend comes from digital foundations in basic education. UNESCO's guidance and global evidence syntheses support this sequencing and the emphasis on teacher capacity, digital content, and safe learning environments.

1.3 Theory of Change and Impact Pathway

Inputs. The Mission mobilises (i) legal instruments and governance bodies (Host Country Agreement; SUDESA and DTIF charters), (ii) financing via a rules-based facility with IPSAS reporting, ESF/ISS

safeguards, and OCDS disclosure, and (iii) technical standards and architectures (NIST CSF 2.0, ISO/IEC 27001:2022, ID4D design principles).

Activities. Government modernisation: migrate to enterprise-grade collaboration, identity, and records; institute Zero-Trust; implement e-services and open data. Education: connect campuses and schools, deploy device and management solutions, train educators, and adopt curriculum-aligned digital resources. Broadband: build neutral fibre to buildings/compounds and community nodes; wholesale access for multiple ISPs; integrate satellite/fixed-wireless for remote areas; enforce wayleave and right-of-way frameworks. Procurement and safeguards: publish OCDS datasets across all projects; apply ESF/ISS screening and instruments; operate grievance and incident protocols.

Outputs. Functioning sovereign collaboration and document systems across core ministries; operational security operations centre with incident response; connected universities/TVET institutions and initial school clusters; live open-access wholesale marketplaces at community/building level; end-to-end public procurement disclosure; cleared safeguards instruments and complaint mechanisms.

Outcomes (3–6 years).

1. **Governance efficiency and trust:** reduced reliance on insecure channels; improved records integrity and service turnaround times; external audit readiness under ESF/ISS/IPSAS regimes.
2. **Human capital and inclusion:** higher tertiary completion and employability linked to digital skills; progressive expansion of digital learning in basic education with teacher support and safe-use protocols.
3. **Connectivity and competition:** greater retail ISP choice and lower entry barriers via neutral-host fibre; improved coverage through complementary satellite/wireless; measurable price/quality improvements consistent with Swedish open-access precedents.

Impacts (7–10 years). A **digitally sovereign state** with resilient public services and data protection grounded in Malabo-consistent legislation; a **more inclusive digital economy** with higher participation of SMEs and youth; and a **measurable narrowing of the digital divide**, reflected in penetration and quality indicators tracked through the GovTech and education results frameworks.

Assumptions and Risk Management. Success presumes high-level political sponsorship; stable DTIF financing; and timely enactment of data-protection, digital identity, cybersecurity, and e-procurement statutes. Risks—vendor lock-in, cyber incidents, inequitable access, or procurement capture—are mitigated through technology neutrality (ID4D), Zero-Trust security (NIST/ISO), open contracting (OCDS), and risk-based ESF/ISS safeguards with grievance, incident, and audit mechanisms.

Alignment. The pathway is explicitly mapped to **Agenda for Social Equity 2074**, while operational convergence with the AU’s **Digital Transformation Strategy** and the Malabo Convention anchors continental legitimacy and donor confidence.

[Digital 2023: South Sudan — DataReportal – Global Digital Insights](#)

[Individuals using the Internet \(% of population\) - South Sudan | Data](#)

[Statistics](#)

[GTMI](#)



[Broadband Infrastructure, Access and Use](#)

[Digital learning and transformation of education | UNESCO](#)

[EdTech in Developing Countries: A Review of the Evidence | The World Bank Research Observer | Oxford Academic](#)

[The Digital Transformation Strategy for Africa \(2020-2030\) | African Union](#)

[African Union Convention on Cyber Security and Personal Data Protection | African Union](#)

[Environmental and Social Framework \(ESF\)](#)

[African Development Bank Group's Updated Integrated Safeguards System \(ISS\) Becomes Effective | African Development Bank Group](#)

[The NIST Cybersecurity Framework \(CSF\) 2.0](#)

[Cybersecurity Framework | NIST](#)

[PRINCIPLES | Identification for Development](#)

[Principles | Identification for Development](#)

[Open Contracting Data Standard — Open Contracting Data Standard 1.1.5 documentation](#)

[World Bank Document](#)

[Reports and studies - Stokab](#)

[Cold wind of competition blows through Swedish municipal fibre networks](#)

[Digital connectivity in Sweden | Shaping Europe's digital future](#)

2. Mission Objectives and Success Criteria

2.1 Strategic Objectives

The Mission advances three interdependent strategic objectives that together constitute a coherent pathway from foundational state capability to inclusive growth and social equity.

Objective 1 — Digital Sovereignty and Governance Integrity.

South Sudan shall establish a sovereign, interoperable, and secure digital backbone for public administration that enables policy coherence, lawful processing of data, and continuous service delivery. Security and resilience will be operationalised through a **Zero-Trust** posture aligned to the **NIST Cybersecurity Framework 2.0** and its governance-and-risk constructs ([NIST CSF 2.0](#); [CSF 2.0 white paper](#)). Information-security management will be progressively formalised under **ISO/IEC 27001:2022** ([ISO/IEC 27001](#)), with road-mapped certification for designated entities. Procurement and fiduciary integrity will be evidenced via structured, end-to-end disclosure under the **Open Contracting Data Standard (OCDS)**, improving competition and enabling value-for-money analytics ([OCDS documentation](#); [World Bank open-contracting note](#)). Environmental and social risk management will apply the **World Bank Environmental and Social Framework (ESF)** and the **African Development Bank's updated Integrated Safeguards System (ISS)** effective **31 May 2024** ([World Bank ESF](#); [AfDB ISS press release, 4 Jun 2024](#)).

Objective 2 — Educational Equity and Human Capital Development.

The education track will be phased: short-term digitalisation of universities and TVET to strengthen the workforce pipeline, followed by medium- to long-term integration in primary and secondary schooling to secure intergenerational equity. This sequencing reflects international evidence that **instruction-enhancing and self-led digital learning interventions** are most consistently associated with learning gains in developing-country contexts, whereas device access alone is insufficient ([World Bank—EdTech evidence review](#); [UNESCO—digital learning policy page](#)). Teacher capacity, curriculum alignment, safe-use protocols, and accessibility accommodations will be embedded to avoid exacerbating inequalities ([UNESCO](#)).

Objective 3 — Inclusive Connectivity and Economic Participation.

The broadband strategy adopts a **neutral-host, open-access** model, separating passive infrastructure from active operations and retail service, thereby lowering entry barriers and enabling ISP competition. Sweden’s municipal open-access model (e.g., **Stokab**) demonstrates that wholesale-only, non-discriminatory dark-fibre networks can catalyse FTTP coverage, lower costs, and stimulate innovation when paired with appropriate governance ([Stokab reports & studies](#); [Analysys Mason—Swedish municipal fibre networks](#)). This supply-side design complements demand-side measures and aligns with Sweden’s national connectivity policy for ubiquitous, high-quality access ([European Commission—Digital connectivity in Sweden](#)).

Collectively, these objectives align with the **Agenda for Social Equity 2074** and with continental standards set by the **African Union Digital Transformation Strategy (2020–2030)** and the **Malabo Convention** on cybersecurity and personal-data protection ([AU Digital Strategy](#); [AU Malabo Convention—treaty text](#)).

2.2 Operational Objectives

2.2.1 Digital Government Enablement

Objectives.

(a) Migrate core executive and fiscal ministries to a sovereign collaboration, identity, and records environment; (b) implement Zero-Trust controls and establish a national SOC; (c) operationalise a shared e-Government platform and digital public goods (identity, registries, payments) consistent with **ID4D** Principles on inclusion, technology-neutrality, and rights-based governance ([ID4D Principles](#); [ID Principles site](#)).

Expected Outputs.

— Microsoft 365 Government and Azure-based services rolled out across priority ministries; SOC with incident handling and SLAs; policy stack for data classification, DPIA triggers, and breach notification aligned to Malabo Convention principles; enterprise architecture and interoperability profiles for identity/registry services ([NIST CSF 2.0](#); [ISO/IEC 27001](#); [Malabo](#)).

Impact Pathway.

Risk-reduced state operations; improved service turnaround; audit-ready information governance under ESF/ISS; measurable reduction in insecure channels and ad-hoc data handling ([World Bank ESF](#); [AfDB ISS](#)).

2.2.2 Education Digitalisation

Objectives.

(a) Connect and digitalise all public universities/TVET; (b) deploy managed devices and learning platforms with classroom analytics; (c) build teacher digital competencies and accessible content

pipelines; (d) progressively integrate digital curriculum in basic education (with rural first-mover clusters). Evidence-informed design will prioritise instructional quality, teacher support, and accessible modalities ([EdTech evidence—WB](#); [UNESCO guidance](#)).

Expected Outputs.

— University and TVET networks with campus Wi-Fi and identity federation; managed device pools with MDM; teacher CPD programmes; safeguarding and online-safety protocols; inclusive content aligned to national curriculum (with accommodations for learners with disabilities) ([UNESCO](#)).

Impact Pathway.

Short-term: improved tertiary readiness of teachers, health workers, and civil servants; Medium-term: rising basic-education digital literacy, attendance, and progression indicators; Long-term: higher employability and entrepreneurship rates among youth.

2.2.3 Open-Access Broadband Deployment

Objectives.

(a) Adopt a national open-access policy and regulatory framework; (b) deploy **neutral-host fibre** to buildings/compounds and community nodes; (c) integrate satellite and fixed-wireless for remote areas; (d) institute standard wayleave/rights-of-way and building-code provisions for fibre-ready MDU risers; (e) operate a wholesale marketplace admitting multiple ISPs on non-discriminatory terms ([Stokab studies](#); [Analysys Mason](#)).

Expected Outputs.

— Dark-fibre laterals to MDUs/public facilities; communications-operator layer for active equipment; wholesale product catalogue and SLAs; integrated national broadband map and address registry ([EU page on Sweden's mapping tools](#)).

Impact Pathway.

Increased retail ISP competition; lower retail prices per Mbps; coverage extension to underserved localities; platform for smart-services ecosystems (e-health, agritech, MSME digitisation).

2.2.4 Legal, Institutional, and Compliance Objectives

Objectives.

(a) Draft and enact priority laws: **Data Protection and Privacy Act**, **Cybersecurity/CERT Law**, **Digital Identity Act**, and **Digital Procurement/e-GP (OCDS) Reform**; (b) operationalise DTIF fiduciary controls (IPSAS reporting, independent audit); (c) embed **OCDS** publication and ESF/ISS safeguards across the portfolio ([Malabo](#); [OCDS](#); [World Bank ESF](#); [AfDB ISS](#)).

Expected Outputs.

— Laws enacted with implementing regulations; national CERT/CSIRT designated and linked to SOC; facility-wide disclosure and grievance mechanisms operational.

2.3 Key Performance Indicators and Targets (Multi-Tier Results Framework)

Notes. Baselines will be confirmed during the 90-day MEL inception. Where national statistics are unavailable, internationally recognised proxies will be applied (e.g., **DataReportal** for initial internet-use estimates; **World Bank GTMI** for comparators) ([Digital 2023 South Sudan](#); [World Bank—GTMI](#)).

**Impact-level (10-year horizon)**

Impact Area	Indicator	Baseline (indicative)	Year 10 Target	Sources & Methods
Digital inclusion	Individuals using the internet (% of population)	~7% (2023)	≥ 80%	National ICT survey; triangulate with WB, DataReportal
Governance integrity	Central ministries with ISO/IEC 27001-certified ISMS	0	≥ 15 entities	Certification records; ISO/IEC 27001
Education equity	Primary schools with digital curriculum & teacher training	~0	≥ 70%	MoE administrative data; QA by independent verification; UNESCO
Market competition	Average retail price per Mbps (USD)	High/unknown	≥ 60% reduction	National price basket; consumer panels; OECD-style method; benchmark to open-access cases (Analysys Mason ; Stokab)

Outcome-level (3–6-year horizon)

Outcome Domain	Indicator	Y3	Y6	Sources & Methods
GovTech enablement	Core ministries on Microsoft 365 Government & Azure tenancy	5	All central	Administrative records; alignment to GTMI focus areas
Cyber resilience	National SOC live; % of high-risk entities under 24/7 monitoring	SOC live; ≥ 40%	≥ 80%	SOC logs; NIST CSF 2.0 maturity profiles
e-Services	Priority services live (civil registry, tax, business, land, social protection)	≥ 5	≥ 15	Service catalogues; time-to-deliver metrics
Higher education	Public universities/TVET connected; managed devices deployed	100% / 20k	Sustained / 50k	MoE/HE data; independent audits; evidence-informed design (WB EdTech)
Basic education	Primary schools using digital curriculum (with trained teachers)	10%	30%	School EMIS; UNESCO methodologies (UNESCO)

Outcome Domain	Indicator	Y3	Y6	Sources & Methods
Connectivity	Premises (MDUs/public) passed by neutral-host fibre (cumulative)	500	5,000	Build certificates; regulator mapping (EC page)
ISP competition	ISPs active on wholesale platform	≥ 5	≥ 12	Platform registry; OECD competition metrics
Procurement transparency	Share of DTIF-funded contracts published in OCDS (planning→implementation)	100%	100%	OCDS pipelines; OCDS
Safeguards compliance	Activities screened and instrumented per ESF/ISS	100%	100%	Screening logs; instrument repositories (ESF ; ISS)

Output-level (annual/short-term)

Output	Indicator & Annual Targets (illustrative)	Sources
Governance controls	Data classification policy, DPIA regime, breach notification protocol adopted in Y1; annual staff completion ≥ 90%	Policy registry; training logs
SOC readiness	Tiered monitoring playbooks; quarterly incident drills; MTTR < 24 h by Y2	SOC reports; NIST CSF 2.0
Education enablement	University networks and MDM live; ≥ 2,000 teachers certified per year; inclusive content repository launched	MoE/HE admin; UNESCO guidance
Broadband build	≥ 200 nodes/year (Y1–Y3), ≥ 1,000/year (Y4–Y6) subject to CAPEX; wayleave SLAs ≤ 30 days	Build logs; regulator filings
Open contracting	OCDS releases at planning, tender, award, contract, implementation; standstill & debrief observed per thresholds	Procurement platform; OCDS
Safeguards/MEL	100% screening; GRM live; QPR and ARR published to portal	ESF/ISS trackers; MEL portal

Inclusion Disaggregation. For all relevant indicators: sex, age, disability, and rural/urban will be disaggregated per ESF guidance; education indicators will track teacher and learner participation by gender and location ([World Bank ESF](#); [UNESCO](#)).

2.4 Success Criteria and Conditions for Sustainability

Institutionalisation. Durable success is evidenced when (i) legal frameworks (data protection, cybersecurity/CERT, digital identity, e-procurement/OCDS) are enacted and in force; (ii) DTIF fiduciary

controls produce timely **IPSAS**-compliant reports and unqualified independent audits; (iii) SUDESA's governance (JSC/DTSC) operates with documented policies, minutes, and disclosure; and (iv) national CERT and SOC maintain continuous operations with measured incident response ([ESF](#); [AfDB ISS](#); [OCDS](#)).

Financial Sustainability. The facility's cost-recovery and administrative arrangements must (a) remain compatible with donor norms; (b) disclose fee schedules and indirect rates annually; and (c) maintain treasury policies for liquidity and risk consistent with public-sector audit principles. Performance-based co-financing from development partners should be tied to compliance (OCDS, ESF/ISS) and results (KPIs) ([OCDS](#); [ESF](#)).

Social Licence and Trust. Public acceptance will be built through (a) rights-based ID systems adhering to **ID4D** Principles; (b) robust privacy-by-design, DPIAs, and lawful redactions in disclosure; (c) accessible grievance and remedy mechanisms for citizens and contractors; and (d) regular publication of performance dashboards ([ID4D Principles](#); [OCDS](#)).

Risk Mitigation and Adaptation.

- **Vendor lock-in:** mandate open standards, portability clauses, and phased competition; align to ID4D's technology neutrality ([ID4D](#)).
- **Cyber incidents:** continuous improvement against **NIST CSF 2.0** profiles; ISO 27001 controls; drills; lessons-learned loops ([NIST CSF 2.0](#); [ISO/IEC 27001](#)).
- **Safeguards lapses:** independent reviews for high-risk activities; SEA/SH protocols with 48-hour serious-incident reporting under ESF/ISS ([ESF](#); [AfDB ISS](#)).
- **Connectivity inequity:** universal-service targeting, wholesale price caps where justified, and community node prioritisation informed by baseline mapping ([EC page—Sweden mapping](#)).

2.5 Alignment with Global and Regional Frameworks

Agenda for Social Equity 2074 (SGGs).

- **SGG 1 (Universal Access):** broadband coverage, e-services, and inclusive access KPIs.
- **SGG 4 (Education & Lifelong Learning):** digital curriculum, teacher CPD, and accessible content KPIs.
- **SGG 8 (Fair Governance):** Zero-Trust controls, ISO 27001 roadmaps, open contracting disclosure.
- **SGG 17 (Ethical Technology):** data-protection law, DPIA regime, ID4D-conformant identity.

AU Agenda 2063 & Digital Strategy (2020–2030).

The Mission operationalises AU priorities for secure, affordable broadband, trusted digital public services, and harmonised data frameworks ([AU Digital Strategy](#)).

Malabo Convention.

Cybersecurity and personal-data provisions provide the treaty-level baseline for legal drafting and institutional mandates ([Malabo Convention text](#)).

World Bank GovTech & ID4D; AfDB Safeguards; Open Contracting.

Design choices, MEL, and disclosure align to **GTMI** focus areas, **ID4D** Principles, **ESF/ISS**, and **OCDS** to ensure donor compatibility and objective assurance ([GTMI](#); [ID4D Principles](#); [ESF](#); [AfDB ISS](#); [OCDS](#)).

2.6 Calculation Notes and Verification

1. **Internet-use and broadband penetration** will rely on national ICT surveys; until established, they will be triangulated with international datasets ([World Bank series](#); [DataReportal—South Sudan](#)).



2. **Security maturity** will be assessed against **NIST CSF 2.0** Profiles and ISO 27001 control adoption; third-party audits will verify selected entities ([NIST CSF 2.0](#); [ISO/IEC 27001](#)).
3. **Open contracting** compliance requires OCDS release packages at each stage; automated validators and independent data-quality reviews will be applied ([OCDS docs](#)).
4. **Safeguards** performance will record screening/classification and instrument delivery under **ESF/ISS**, with disclosed GRM statistics and incident logs ([ESF](#); [AfDB ISS](#)).
5. **Education outcomes** will include teacher-training completion and digital-curriculum adoption rates; alignment to evidence-based practices will be documented ([World Bank—EdTech review](#); [UNESCO](#)).

3. Implementation Strategy and Phasing (10-Year Programme)

3.1 Programme Architecture and Decision Rights

Implementation is organised as a portfolio of coordinated workstreams—Digital Government, Education Digitalisation, Open-Access Broadband, and Legal/Compliance—under the SUDESA Secretariat, governed by the Joint Steering Committee (JSC) for strategy and fiduciary oversight and by the Digital Transformation Steering Committee (DTSC) for technical assurance and stage-gates. All portfolio items will comply with: (i) NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022 for security and information-risk management; (ii) Open Contracting Data Standard (OCDS) for end-to-end procurement disclosure; and (iii) World Bank ESF and AfDB ISS (effective 31 May 2024) for environmental and social safeguards. These frameworks provide the normative guardrails and eligibility conditions for concessional finance and co-financing ([NIST CSF 2.0](#); [ISO/IEC 27001:2022](#); [OCDS](#); [World Bank ESF](#); [AfDB ISS—4 Jun 2024 press release](#)).

The programme’s strategic alignment is explicit: Agenda for Social Equity 2074; AU Digital Transformation Strategy (2020–2030) for secure, affordable broadband and harmonised data frameworks; and the Malabo Convention for cybersecurity and personal-data protection ([AU Digital Strategy](#); [Malabo Convention](#)).

3.2 Phasing Overview (Years 1–10)

The ten-year horizon is structured into three sequential, partially overlapping phases, with staged capacity transfer and increasing domestic ownership.

Phase I (Years 1–3): Foundational Enablement and Early Scale.

Government foundations are stood up: sovereign collaboration and identity, Zero-Trust baselining, national Security Operations Centre (SOC), and first e-services. Universities/TVET are connected and digitalised; device programmes and teacher capacity building begin. Open-access fibre starts with public institutions, MDUs and community nodes in priority urban corridors, with satellite/fixed-wireless backstopping remote areas; the wholesale marketplace launches. Legal workstreams table data-protection, cybersecurity/CERT, digital identity and e-procurement/OCDS bills. All contracting transitions to OCDS publication and risk-based safeguards under ESF/ISS ([NIST CSF 2.0](#); [ISO/IEC 27001](#); [OCDS](#); [ESF](#); [ISS](#)).

Phase II (Years 4–6): Expansion, Integration, and Market Deepening.

E-Government expands to 10–15 high-demand services with digitised registries and payments. ISO 27001 roadmaps mature across ministries; SOC coverage extends to high-risk state-owned and critical-sector entities. Primary-school digitalisation scales in cluster waves with teacher CPD, inclusive



content, and connectivity to schools via a mix of fibre and wireless. Open-access fibre passes 5,000 nodes; ISP participation increases as wholesale pricing and SLAs stabilise. Legal instruments enactment is completed and regulators operationalise e-procurement and data-protection supervision in line with Malabo and AU strategy ([AU Digital Strategy](#); [Malabo](#)).

Phase III (Years 7–10): Consolidation, Optimisation, and Handover.

Focus shifts to resilience, performance, and lifetime value: optimisation of e-services and identity, ISO certifications in priority entities, curriculum deepening and assistive technologies at scale, and wholesale broadband saturation in provincial and rural markets using neutral-host fibre complemented by satellite and fixed-wireless. Full institutionalisation of fiduciary, safeguards, and disclosure regimes is evidenced in IPSAS-compliant reporting, unqualified external audits, and independent evaluations; long-term O&M, tariff, and service-level governance are embedded in national systems ([World Bank ESF](#); [OCDS](#)).

3.3 The First 90 Days and Year 1 Milestones

A disciplined start eliminates ambiguity, builds momentum, and sets compliance baselines.

Days 0–30 (Mobilisation).

Issue convening notices for the inaugural DTSC/JSC; adopt interim data-classification, DPIA triggers, and breach notification; approve SOC concept of operations; publish the portfolio-wide OCDS disclosure protocol; launch legal drafting calendars for data-protection and e-procurement; settle the first Annual Work Plan & Budget (AWPB) and procurement plan in DTIF format ([OCDS](#); [ESF](#)).

Days 31–60 (Technical baselining).

Stand up the Microsoft 365 Government tenancy and identity, pilot Zero-Trust controls in two core ministries, and complete SOC facility site selection. Finalise open-access reference design, including the three-layer neutral-host model (owner – communications operator – retail ISP) drawing on Swedish practice; pre-procure survey and design for the first 200 nodes ([Analysys Mason—Swedish model](#); [Stokab studies](#)).

Days 61–90 (Procurement and safeguards).

Tender SOC tools and services and the first broadband works/active equipment using open competition; publish planning and tender releases in OCDS; complete ESF/ISS screening for all Year 1 packages; launch the public MEL portal and the grievance redress mechanisms for communities and workers ([OCDS](#); [AfDB ISS](#)).

Year 1 Milestones.

SOC “minimum viable” monitoring live for 3–5 entities; five universities fully connected and operating Microsoft 365 Education; 200 neutral-host nodes built and lit; data-protection and e-procurement/e-GP bills tabled; 100% DTIF awards disclosed in OCDS across all five stages (planning → implementation) ([NIST CSF 2.0](#); [UNESCO digital education](#); [OCDS](#)).

3.4 Stage-Gates and Decision Thresholds

All major packages pass standard gates, documented by DTSC technical opinions and JSC resolutions:

- **Gate 0: Portfolio Readiness.** Enterprise architecture approval; safeguards classification; OCDS publication pipeline verified ([ESF](#); [OCDS](#)).



- **Gate 1: Procurement Clearance.** Competition strategy, lotting, evaluation criteria, and risk mitigations consistent with **World Bank Procurement Regulations (Nov 2020)** (WB Procurement Regs).
- **Gate 2: Security & Privacy Readiness.** Zero-Trust controls baselined, DPIA completed where personal data involved; incident-response plans aligned to NIST/ISO ([NIST CSF 2.0](#); [ISO/IEC 27001](#)).
- **Gate 3: Go-Live Authorisation.** Acceptance criteria met; service levels and monitoring configured; GRM active; OCDS award/contract/implementation releases posted.
- **Gate 4: Benefits Realisation.** Outcome KPIs validated; lessons-learned captured; optimisation backlog agreed.

3.5 Workstream Roadmaps

A. Digital Government.

Years 1–2: migrate five core ministries; SOC live; first five e-services (civil registry, tax, business registration, land records, social protection). Years 3–6: expand to all central ministries; integrate identity, registries, and payments; ISO roadmaps published for 10–15 entities. Years 7–10: ISO certifications achieved in priority entities; advanced analytics and open-data services mature with privacy-by-design controls ([NIST CSF 2.0](#); [ISO/IEC 27001](#)).

B. Education Digitalisation.

Years 1–3: all public universities/TVET connected; managed device pools; teacher CPD cohorts; inclusive content repository. Years 4–6: cluster-based rollout to 30% of primary schools; learning-management and classroom analytics; local content creation incentives. Years 7–10: 70% of schools integrated; assistive technologies scaled; continuous CPD and school-level digital safety embedded ([UNESCO](#); [WB EdTech evidence](#)).

C. Open-Access Broadband.

Years 1–3: adopt open-access policy and wholesale product catalogue; build 500 neutral-host nodes; launch the wholesale marketplace. Years 4–6: scale to 5,000 nodes; expand ISPs to ≥ 12 ; codify wayleave/building-code fibre-ready standards. Years 7–10: rural/peri-urban saturation using fibre plus satellite/fixed-wireless; performance-based maintenance; universal-service targeting data-driven by mapping and demand aggregation ([Analysys Mason](#); [Stokab](#)).

D. Legal and Compliance.

Years 1–3: enact data-protection/privacy, cybersecurity/CERT, digital identity, and e-procurement/OCDS statutes; stand up the data-protection authority and CERT. Years 4–6: secondary regulations and supervision; case handling; sanctions and remedies practice. Years 7–10: periodic reviews and cross-border coordination; alignment to AU instruments and Malabo updates ([Malabo](#); [OCDS](#)).

3.6 Resourcing and Capacity Transfer

A mixed staffing model blends international expertise with structured localisation. The Secretariat operates a lean PMO with embedded fiduciary, safeguards, and disclosure specialists; SOC and CERT recruit national analysts with vendor-supported training, aligned to NIST/ISO frameworks. Education relies on “train-the-trainer” cascades and CPD credits; broadband uses owner’s engineers for quality assurance while growing national O&M teams. By Year 6, $\geq 70\%$ of specialist roles are national; by Year 10, all steady-state roles are institutionalised ([NIST CSF 2.0](#); [ESF](#)).



3.7 Financing, Disbursement, and Cost Recovery

The DTIF finances capital works, software and licensing, managed services, TA, and MEL. Disbursements use direct payments, reimbursements, and advances with IPSAS-compliant IFRs and unqualified independent audits; negative lists and eligibility rules apply. Administrative fees, indirect rates, and cost-recovery schedules are disclosed annually; waivers require JSC resolution. Safeguards and OCDS publication are conditions precedent for disbursement tranches ([World Bank ESF](#); [OCDS](#)).

3.8 Procurement Strategy and Vendor Neutrality

Open competitive procedures are the default; lotting lowers barriers to entry and encourages SME participation. Technical specifications mandate open standards and interoperability; data-portability and exit clauses prevent lock-in, consistent with ID4D design principles. All contracting data and documents are published across planning, tender, award, contract, and implementation stages in OCDS, with standstill and debrief protocols per thresholds (WB Procurement Regulations, Nov 2020; [ID4D Principles](#); [OCDS](#)).

3.9 Risk Management and Contingencies

Cyber risk is mitigated through continuous improvement against NIST CSF 2.0 profiles, ISO controls, exercises, and third-party testing. Safeguards risks—SEA/SH, land, community health and safety—trigger proportionate instruments and independent reviews under ESF/ISS; serious incidents are notified within 48 hours. Market risks (low ISP participation) are hedged via transparent wholesale pricing, service credits, and demand aggregation. Legal risks are reduced through phased enactment and operational supervision capacities ([NIST CSF 2.0](#); [ESF](#); [AfDB ISS](#)).

3.10 Ten-Year Timeline

Years 1–2: SOC established; five core ministries migrated; five e-services live; universities/TVET connected; 200–500 open-access nodes; priority bills tabled/enacted.

Years 3–4: All central ministries migrated; ISO roadmaps published; cluster-based primary rollouts begin; 1,500–2,500 nodes; marketplace admits 5–8 ISPs; supervisory authorities functional.

Years 5–6: 30% schools integrated; 5,000 nodes; ≥ 12 ISPs; e-services reach 10–15; initial ISO certifications.

Years 7–8: Rural saturation with fibre plus satellite/wireless; education assistive technologies scaled; optimisation of e-services and registries.

Years 9–10: 70% schools integrated; 10,000 nodes; advanced analytics and open data with privacy-by-design; full fiduciary and safeguards institutionalisation evidenced in audits and evaluations ([UNESCO](#); [OCDS](#)).

3.11 Exit, Handover, and Sustainability

Exit is defined by: (i) statutory and institutional autonomy of regulators and CERT; (ii) certified security management in priority entities; (iii) cost-recovery for wholesale networks covering O&M and capex renewal; (iv) stable CPD pipelines for teachers and civil servants; (v) MEL dashboards and OCDS publication continuing under national ownership; and (vi) periodic legal reviews aligned to AU instruments and Malabo updates ([ISO/IEC 27001](#); [AU Digital Strategy](#); [Malabo](#)).

4. Institutional Architecture and Decision Rights

4.1 SUDESA Secretariat and Core Departments

Purpose and accountability. The SUDESA Secretariat is the executive arm responsible for programme delivery, fiduciary management, safeguards, disclosure, and institutional learning. It is led by an Executive Director (ED), supported by up to two Deputy Executive Directors (DEDs) with portfolios (e.g., Programmes & Operations; Corporate Services & Governance). The Secretariat is accountable to the Joint Steering Committee (JSC) for strategy, resources, and performance, and provides the Digital Transformation Steering Committee (DTSC) with technical documentation and stage-gate dossiers. Financial management follows IPSAS, internal control aligns with COSO and internal-audit practice under IIA Standards, and assurance is framed by INTOSAI ISSAI 100 for public-sector oversight (IPSAS: <https://www.ipsasb.org/publications/2024-handbook-international-public-sector-accounting-pronouncements> COSO: <https://www.coso.gov/wp-content/uploads/2021/12/COSO-2013.pdf> IIA Standards: <https://www.theiia.org/en/content/guidance/mandatory/standards/international-standards-for-the-professional-practice-of-internal-auditing> ISSAI 100: <https://www.issai.org/wp-content/uploads/2019/08/ISSAI-100-Fundamental-Principles-of-Public-Sector-Auditing-1.pdf>

Executive Office. Strategic planning, portfolio management office (PMO), partnerships, communications, records, disclosure portal, and business continuity.

Eight Core Departments (mandates and interfaces).

1. **Digital Transformation & Systems (DTS).** Enterprise architecture, interoperability standards, identity/registry platforms, infrastructure/cloud, SOC design and operations, Zero-Trust security and incident response aligned with NIST CSF 2.0 and ISO/IEC 27001:2022 (NIST CSF 2.0: <https://www.nist.gov/cyberframework> ISO/IEC 27001: <https://www.iso.org/standard/27001> . DTS provides the DTSC with technical opinions at each stage-gate and ensures privacy-by-design DPIAs for data-intensive systems.
2. **Agriculture, Food Security & Rural Livelihoods (AFRL).** Digital agriculture integration with sector programmes; interfaces to registries, market and logistics platforms; safeguards coordination for agri-infrastructure under **ESF/ISS** (World Bank ESF: <https://www.worldbank.org/en/projects-operations/environmental-and-social-framework> AfDB ISS—effective 31 May 2024: <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>
3. **Social Development & Inclusion (SDI).** Citizen-centred design and accessibility across e-services and education rollouts; rural and vulnerable-group targeting; stakeholder engagement consistent with ESF's disclosure and GRM principles (ESF: link above).
4. **Gender Equity & Safeguards (GES).** Environmental and social screening/classification; instruments (ESIA/ESMP, LMP, SEP, RAP as relevant); SEA/SH protocols with 48-hour serious-incident reporting; independent reviews for high-risk activities under ESF/ISS (ESF/ISS links above).
5. **Finance, Treasury & Fiduciary (FTF).** IPSAS accounting; AWPB preparation; IFRs and annual financial statements; treasury and cost-recovery administration; external audit procurement



and liaison; internal-control framework per **COSO** and assurance mapping per **INTOSAI** (IPSAS/COSO/ISSAI links above).

6. **Procurement & Open Contracting (POC).** Procurement planning and execution under the **World Bank Procurement Regulations (Nov 2020)**; end-to-end publication in **OCDS**; complaints handling, standstill/debriefing, sanctions screening and beneficial-ownership disclosures

WB Procurement Regs: <https://thedocs.worldbank.org/en/doc/178331533065871195-0290022020/original/ProcurementRegulations.pdf> OCDS: <https://standard.open-contracting.org/latest/en/> .

7. **Legal, Governance & Compliance (LGC).** Legal advisory; policy and statute drafting (data-protection, cybersecurity/CERT, digital identity, e-procurement/open-contracting) aligned with AU Malabo Convention and ID4D Principles; conflicts-of-interest registers; whistleblowing/anti-retaliation mechanisms (Malabo: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> ID4D Principles: <https://id4d.worldbank.org/guide/1-principles>
8. **Monitoring, Evaluation, Learning & Research (MELR).** Theory of change, multi-tier results framework, disaggregation (sex/age/disability/rural-urban), verification and evaluations; public dashboards; linkage of performance data to procurement (OCDS ocid) and safeguards (ESF/ISS) (OCDS/ESF/ISS links above).

Each Department Director is accountable for delivery, compliance, and data quality; cross-cutting committees (e.g., Data Governance Board; Risk & Continuity Forum) are chartered with clear decision rights and reporting to the ED and JSC.

4.2 Digital Transformation Steering Committee (DTSC)

Purpose and remit. The DTSC is the technical governance body for digital transformation. It sets and updates the enterprise architecture, security and data-governance standards, clears programme designs, and issues formal stage-gate opinions before procurement and go-live. Its directives are grounded in widely accepted frameworks—NIST CSF 2.0 for cybersecurity, ISO/IEC 27001:2022 for information-security management, and ID4D for rights-based identity design (NIST/ISO/ID4D links above).

Composition and chairing. Senior representatives from the ministry in charge of ICT/digital government, Ministry of Finance and Planning, the ED of SUDESA, Directors of DTS and POC, an LGC representative, and one EUSL executive appointee. The DTSC is co-chaired by a Government representative and an EUSL representative to ensure balanced decision-making.

Functions.

1. Approve and publish technical standards (interoperability, API policies, cloud profiles, SOC runbooks, Zero-Trust patterns).
2. Clear designs for digital public infrastructure (identity, registries, payments) after DPIA and security reviews.
3. Operate the stage-gate system (Gate 0–4) to ensure readiness on security, privacy, safeguards, procurement and disclosure before commitments (see §3.4; WB Procurement Regs & OCDS above).



4. Verify OCDS publication pipelines are configured for each contracting process and that ESF/ISS screening outcomes are recorded.
5. Monitor technical performance and cyber incidents; require corrective actions; escalate systemic risks to the JSC (NIST CSF 2.0/ISO 27001).

Procedures and records. Quorum, meeting cadence, agenda circulation, minutes, and decision registers are codified. Non-confidential directives and minutes are disclosed per the Disclosure Policy; privacy and security redactions are justified and logged (ESF disclosure principles; OCDS).

4.3 Joint Steering Committee (JSC)

Purpose and remit. The JSC is the supreme decision-making and oversight body for strategy, resources, policy adoption, and assurance. It approves the multi-year strategy and AWPB, portfolio and major contract awards above delegated thresholds, institutional policies (fiduciary, procurement/open-contracting, safeguards, data governance), and manages oversight through subcommittees. Its assurance model references INTOSAI ISSAI 100, IIA Standards, and the COSO internal-control framework to ensure legality, transparency, probity, and performance (ISSAI/IIA/COSO links above).

Composition and chairing. Government and EUSL appointees in equal number; **co-chaired** (one per Party). Observers from development partners/regulators may be invited, subject to confidentiality and avoidance of conflicts.

Core decision rights.

- a) **Strategy & Budget:** approve multi-year strategy and AWPB; set portfolio priorities and risk appetite.
- b) **Policy & Control Environment:** adopt and amend financial management, procurement/open-contracting, safeguards, data-governance and disclosure policies.
- c) **Portfolio Governance:** approve or delegate approvals for programmes/projects and contract awards; set prior/post review thresholds per **WB Procurement Regs**; confirm Gate-decision.
- d) **Assurance & Compliance:** receive quarterly IFRs and performance reports; appoint independent **external auditors**; approve internal-audit charters and plans; monitor GRM/SEA-SH/incident statistics (IPSAS/ISSAI/IIA/ESF/ISS).
- e) **People & Organisation:** appoint and evaluate the ED; approve Directors on ED recommendation; confirm organogram.

Subcommittees.

— **Audit & Risk:** external audit independence; IFR timeliness; risk register; control remediation (ISSAI/IIA/COSO).

— **Ethics & Compliance:** conflicts-of-interest and gifts registers; whistleblowing/anti-retaliation; related-party transactions (IIA Standards).

— **Safeguards & Inclusion:** ESF/ISS screening quality; SEA/SH prevention and response; GRM effectiveness (ESF/ISS).

Transparency and records. The JSC maintains minutes and a decision register; non-confidential decisions and procurement data are disclosed in machine-readable formats with OCDS identifiers to enable public scrutiny and linkages to MEL indicators (OCDS: <https://standard.open-contracting.org/latest/en/>).

4.4 Delegations of Authority and Escalation Protocols

Delegations of Authority (DoA). The JSC adopts a Delegation of Authority Matrix that specifies financial, contractual, and administrative thresholds, review modalities, and documentation standards. The matrix embodies:

1. **Commitment authority.** The ED may approve commitments up to a defined ceiling per contract; Department Directors may approve micro-procurements within micro-thresholds; higher values require JSC approval or prior review consistent with WB Procurement Regulations (Nov 2020) (link above).
2. **Contract variations.** Cumulative variation ceilings (e.g., $\leq 15\%$ of original price) are set for management approval; above this, JSC sign-off is required. All variations are published in **OCDS** with justification and updated implementation data (OCDS link above).
3. **Disbursement and treasury.** Dual- or multi-signature controls, beneficiary-change verification, and IPSAS-compliant reconciliations are mandatory (IPSAS link above).
4. **Policies and manuals.** The ED is authorised to issue administrative instructions consistent with JSC-approved policies; conflicts are escalated to the JSC.

Escalation protocols.

— **Technical defects and delivery risk.** The DTSC may issue corrective directives; persistent or systemic non-compliance escalates to the JSC with recommendations (NIST CSF 2.0; ISO 27001).

— **Safeguards and SEA/SH incidents.** Serious incidents are notified within **48 hours**, triggering investigation, survivor-centred protocols, contractor sanctions if applicable, and JSC briefings; summary statistics are disclosed per ESF/ISS (ESF/ISS links above).

— **Integrity and procurement complaints.** The POC runs an independent complaints mechanism with time-bound acknowledgements and decisions; unresolved challenges escalate to an independent review panel; outcomes and debriefs are recorded and published consistent with **WB Procurement Regs** and **OCDS** (links above).

— **Cybersecurity events.** The SOC declares severity levels and coordinates response; critical incidents are escalated to the national **CERT/CSIRT** under the cybersecurity statute; post-incident reviews are required, with lessons captured and tracked (NIST CSF 2.0; ISO 27001; Malabo Convention: link above).

— **Financial and fiduciary breaches.** Material control failures, suspected fraud/corruption, or sanctions hits are escalated to the Audit & Risk Subcommittee; remedies include suspension of disbursements, recovery, debarment referrals, and disclosure of enforcement actions (ISSAI 100; IIA Standards; WB Procurement Regs).

Reserved matters and unanimity. The DoA identifies decisions requiring unanimous JSC consent, including: ED appointment/removal; approval/amendment of the DoA and Disclosure Policy; changes to audit, inspection, or disclosure rights; waiver of privileges; dissolution/merger of SUDESA; and modification of cost-recovery schedules.

Emergency measures. To preserve life, safety, data integrity, or material assets, the ED may adopt interim emergency measures within a specified ceiling and scope; such measures are notified to the JSC within 48 hours and tabled for ratification at the next sitting (NIST CSF 2.0 for cyber incidents; ESF/ISS for community health/safety).

Conflicts of interest and recusals. All governance members and staff submit initial and annual declarations; ad hoc conflicts are disclosed before deliberation; recusals are recorded in minutes. The Ethics & Compliance Subcommittee oversees enforcement (IIA Standards).

Disclosure and recordkeeping. Decisions, contracts, amendments, performance, safeguards instruments, and audits are archived and disclosed in machine-readable form with **OCDS** identifiers, subject to lawful, narrowly tailored redactions for privacy, security, and commercial sensitivity (OCDS; ESF disclosure principles).

5. Digital Government Blueprint (Microsoft Government Solutions)

This Blueprint sets out the technical, legal, and operational design for a sovereign, interoperable, and secure digital state built on Microsoft platforms and open standards. The design choices are anchored in internationally recognised frameworks for cybersecurity and information governance—**NIST CSF 2.0**, **ISO/IEC 27001:2022**, **ID4D**'s rights-based identity guidance, and open contracting and safeguards regimes that guarantee transparency and public trust. The Microsoft stack is deployed in a way that preserves national sovereignty over data while enabling scale, resilience, and continuous compliance.

[World Bank Document](#)

[Open Contracting Data Standard — Open Contracting Data Standard 1.1.5 documentation](#)

[Digital-Economy-SouthSudan-jun22.pdf](#)

[Education and Technology: EdTech Publications](#)

[GovTech Maturity Index \(GTMI\) Data Dashboard](#)

5.1 Enterprise Architecture and Interoperability

The Government's enterprise architecture will be formalised as a layered blueprint that separates presentation, application, and data layers; exposes services through an API gateway and service bus; and enforces interoperability profiles approved by the DTSC. These profiles require open interfaces (REST/JSON), canonical data models, and metadata discipline, with privacy and security controls embedded from the outset. Zero-Trust principles are made explicit at each layer (identity, endpoints, applications, data, infrastructure, networks, and visibility/automation), and the architecture is versioned through a controlled repository with mandatory design reviews and data protection impact assessments for systems that process personal data.

[African Union Convention on Cyber Security and Personal Data Protection | African Union](#)

[Zero Trust Guidance Center | Microsoft Learn](#)

Operationally, ministries will integrate via a national service bus and API management tier, using policy-based mediation (authentication, authorisation, throttling, schema validation) and auditable data-sharing agreements. Security governance and control requirements follow **NIST CSF 2.0** (govern, identify, protect, detect, respond, recover) and are transformed into enforceable controls through the Government's ISO/IEC 27001 ISMS and the Microsoft platform's configuration baselines and monitoring.

5.2 Identity, Access, and Digital ID

A trusted digital identity ecosystem is the foundation of service access, transaction integrity, and citizen consent. Foundational identity (civil registration and national ID) provides the authoritative source of



truth; functional identities (for businesses, professionals, vehicles, land parcels) bind sector registries to foundational attributes through signed, time-stamped assertions. Access to systems and data is mediated by **Microsoft Entra ID** with multi-factor authentication, conditional access (risk- and context-aware), least-privilege roles, and just-in-time administrative elevation. The identity plane, in other words, becomes the primary control plane of Zero Trust, and it is implemented in a rights-preserving manner consistent with **ID4D** (inclusion, design neutrality, and governance/oversight) and with the **Malabo Convention**'s personal-data protection provisions.

Consent management, revocation, and purpose limitation are enforced at the API layer; all access to sensitive records requires explicit scopes, with audit trails appended to the data subject's file. The design supports step-up authentication for high-risk transactions (e.g., land transfer, director change) and verifiable evidence issuance (digitally signed certificates with revocation status), without foreclosing the later adoption of "verifiable credentials" models.

5.3 Microsoft 365 Deployment (Collaboration, Compliance, and Operations)

The Government collaboration environment will be consolidated on Microsoft 365 for enterprise (with E5-class security and compliance), replacing fragmented and insecure tooling with managed identities, unified messaging, and governed records. Exchange Online, Teams, SharePoint, and OneDrive operate under central policy; Microsoft Purview provides sensitivity labels, encryption, data loss prevention, insider-risk management, lifecycle retention, and audit/eDiscovery. These capabilities enable legal holds, disclosure logs, beneficial-ownership and conflicts registries, and enforceable record-retention schedules for public sector compliance.

[The Digital Transformation Strategy for Africa \(2020-2030\) | African Union](#)

[Microsoft 365 E5 Compliance | Microsoft Security](#)

Security telemetry from Microsoft 365 (Defender for Endpoint/Identity/Office, Cloud Apps) is unified in **Microsoft Defender XDR** and streamed to the SOC for correlation, hunting, and automated remediation. Deployment follows the **Zero Trust** guidance for Microsoft 365 (identity hardening, device compliance baselines, conditional access, privileged-access workstations, and information-protection roll-out in waves), with adoption and change-management programmes for civil servants.

[Environmental and Social Framework \(ESF\)](#)

Note on "Government" tenancy options. Microsoft's GCC High and Azure Government environments are designed specifically for U.S. public sector eligibility and are not generally available to other sovereigns; South Sudan will therefore adopt the Microsoft public cloud with Microsoft Cloud for Sovereignty guardrails and national data-centre integration, as described below.

[Cold wind of competition blows through Swedish municipal fibre networks](#)

5.4 Azure Hosting with Sovereign Controls (Hybrid Pattern)

The hosting strategy uses a **hybrid model**: a sovereign national data centre (for highly sensitive systems and low-latency workloads) integrated with Azure's hyperscale capabilities for elasticity, resilience, and innovation. Sovereignty is achieved through **Microsoft Cloud for Sovereignty**—a set of codified guardrails, "Sovereign Landing Zone" blueprints, and transparency controls that apply policy, encryption, and residency constraints across Azure subscriptions. Confidential computing, customer-managed keys (including HSMs), and operator-transparency logs further strengthen sovereign control while retaining the security and scale advantages of the public cloud.



Azure tenancy is configured as an enterprise **landing zone**, with hub-and-spoke networking, private endpoints, managed identities, backup/DR, and infrastructure-as-code pipelines. Where sector regulators require it, operator access can be constrained to pre-approved support paths and logged under the sovereignty transparency features. This approach acknowledges that **Azure Government** is a physically isolated U.S. instance, while non-U.S. governments can achieve comparable safeguards in Azure public cloud using sovereignty controls and policy portfolios.

5.5 Zero-Trust Security Architecture and SOC Operations

Zero Trust is implemented as policy, architecture, and operational practice. Identities are strongly authenticated and continuously assessed; devices are enrolled and evaluated for health; applications are discovered, governed, and restricted by real-time analytics; data is classified, labelled, and protected wherever it travels; infrastructure is hardened and monitored; and the network uses segmentation and encryption. **Microsoft Sentinel** serves as the cloud-native SIEM/SOAR—ingesting signals from Microsoft 365, Azure, identity providers, endpoints, and network telemetry—automating enrichment and containment actions through playbooks while freeing analysts for higher-order investigations.

The SOC is chartered to maintain 24/7 monitoring, threat hunting, and incident response. It publishes playbooks, mean-time-to-detect/resolve targets, and conducts red-team/blue-team exercises. The DTSC issues annual security-configuration baselines and maturity assessments aligned to **NIST CSF 2.0** and the ISO/IEC 27001 control framework.

5.6 Digital Public Services and Citizen Portals (Service Design, Back-Office, and Assurance)

5.6.1 Unified Service and Account Experience

Citizens and businesses will access services through a **single, national portal** that supports multilingual interfaces, accessibility (WCAG 2.1), and mobile-first progressive web applications designed for low-bandwidth contexts. The portal uses the national digital ID for single sign-on and step-up authentication where risk dictates; consent dashboards enable users to see, grant, and revoke data-sharing authorisations. All transactions are logged with immutable, time-stamped evidence and can be exported for legal proceedings when required. The account space presents a consolidated “lifecycle view” (e.g., a household’s benefits, a business’s licences, a farmer’s entitlements), and embeds a grievance redress mechanism integrated with the Government’s safeguards framework.

5.6.2 Civil Registration and Vital Events (CRVS)

Births, deaths, and marriages will be registered end-to-end online or via assisted channels. Identity proofing leverages civil-registry data and authoritative witnesses as needed; successful registrations result in digitally signed certificates bearing verifiable cryptographic evidence and a revocation endpoint. Sensitive attributes are protected with **Microsoft Purview** sensitivity labels and encryption; registrars operate under role-based access with session recording for audit. These records constitute the “source of truth” for downstream services, including education enrolment, social protection, and passports, and are governed by the Data Protection Act aligned to **Malabo Convention** principles.

5.6.3 Revenue and Tax Administration (Registration, Filing, Payment, Enforcement)

Taxpayers (individuals and entities) register and maintain profiles tied to foundational identity and business registers. Returns are filed through guided forms with **pre-population** from payroll, withholding, and customs interfaces; payments accept cards, bank transfers, and mobile money, with a reconciled ledger that posts to the Treasury system. Risk scoring prioritises audits using multi-source

analytics; notices, appeals, and payment plans are managed within the portal. Records are protected with information-protection labels; compliance teams use **Defender XDR** and **Sentinel** telemetry to secure sensitive case data against exfiltration and insider risk. Public procurement and refund contracts are disclosed using **OCDS**, enabling external scrutiny of high-risk flows.

5.6.4 Business Registration and Licensing (Single Window with UBO Disclosure)

Entrepreneurs can form entities, reserve names, appoint directors, and obtain sector licences in one guided sequence. Director appointments are validated against digital ID, and **ultimate beneficial ownership (UBO)** disclosures are collected with legally binding declarations. Licensing authorities issue digitally signed licences with machine-readable terms; expiries trigger notifications. The public can search non-sensitive company data through an open API; procurement awards reference company identifiers and are published in **OCDS** to discourage conflicts of interest. Data access, retention, and redaction rules are codified in the disclosure policy, enforced by **Purview** and audited by the MELR unit.

5.6.5 Land and Property (Cadastre, Transfers, and Securities)

The land cadastre and deeds are digitised with authoritative parcel identifiers and spatial references. Applications for transfer, subdivision, or encumbrance are lodged online, with identity-verified parties and digital signatures; payments are escrowed until registration is complete. Sensitive geospatial and personal data are classified and protected; registrar actions are double-checked (“four-eyes” control) and fully logged. APIs expose non-sensitive parcel attributes for transparency and valuation (subject to privacy rules), and mortgage registrations integrate with banking systems under enforceable service-level agreements and auditability requirements.

5.6.6 Social Protection and Benefits (Targeting, Enrolment, and Payments)

Households apply via the portal or assisted channels; eligibility is determined through transparent rules that may incorporate verified attributes from the civil register, tax status, schooling, disability certification, and geographic vulnerability indexes. Benefit decisions, appeals, and payment schedules are visible in the citizen account; payments are executed to bank or mobile wallets with confirmation receipts. Grievances and safeguarding—including SEA/SH reporting—are integrated with the **ESF/ISS** grievance mechanisms, and anonymised dashboards report caseloads and processing times to the public.

5.6.7 Education and Qualifications (Enrolment, Records, and Credentials)

Parents enrol learners online; schools confirm seats; and student records follow the learner through schooling and into higher education. Examination results and diplomas are issued as cryptographically verifiable records, with learner consent governing disclosure to employers and universities. Teacher assignments, CPD credits, and classroom analytics are managed within secure role scopes. The design aligns with **UNESCO** guidance on digital learning and safe, inclusive administration, and uses **Purview** to protect minors’ data across collaboration and storage.

5.6.8 Cross-Cutting Guarantees (Security, Transparency, Due Process)

All services operate under the Government’s **Zero-Trust** policies and are monitored centrally by the SOC. Procurement data for system build, licences, and managed services are disclosed in OCDS across planning, tender, award, contract, and implementation stages. Environmental and social safeguards screening and instruments are prepared and disclosed in accordance with the World Bank ESF and AfDB ISS; serious incidents are notified within required timeframes and reported publicly in aggregated form. Each service has an explicit statutory basis, published service standards, and an appeals path; the citizen portal embeds these rights and provides status tracking and documented outcomes.

Compliance Mapping (Indicative)

The Blueprint's controls map to (i) **NIST CSF 2.0** functions and categories for cyber-risk governance, (ii) ISO/IEC 27001 Annex A controls for information security management, (iii) ID4D design and governance principles for identification systems, and (iv) **OCDS** disclosure requirements for procurement, with safeguards accountability under the **World Bank ESF** and **AfDB ISS**. Detailed mappings and control matrices are maintained by the DTSC and audited annually.

6. Education Digitalisation Programme (Universities, TVET, Primary and Secondary)

Purpose and framing. This Programme establishes a sovereign, standards-aligned, and evidence-based digital learning system for South Sudan that strengthens higher education, professional and technical training (including IT maintenance and fibre deployment skills), and basic education. It combines robust platforms and connectivity with teacher capacity, inclusive pedagogy, privacy-preserving data governance, and measurable learning outcomes. The design is guided by UNESCO's policy direction on digital learning, and by rigorous evidence showing that instruction-enhancing and self-led learning interventions outperform device-only approaches in developing-country contexts.

6.1 Pedagogical Intent and System Design Principles

The Programme's pedagogy follows three tenets. First, digital technology must augment teaching quality and equitable access, not merely add devices. Second, digital learning must be inclusive by design—accessible to learners with disabilities, use low-bandwidth modalities, and respect multilingual realities. Third, the system must be rights-respecting in its use of learner data and online spaces. These tenets reflect UNESCO's guidance that technology complements and transforms learning when coupled with policy, teacher support, and governance; they also reflect the World Bank's synthesis that platforms which support improved instruction and guided, self-paced learning deliver the most consistent gains.

Architecture for learning comprises: a national education tenant on Microsoft 365 Education with School Data Sync (SDS) for enrolment and class rosters; Teams for Education as the collaboration hub; Intune for Education for device governance; and an enterprise content and assessment layer. Baseline tenant configuration and identity, data, and security controls follow Microsoft's education deployment guidance and are enforced centrally.

6.2 Universities and TVET (with Applied Digital & Fibre Tracks)

Universities. All public universities will be connected and onboarded to Microsoft 365 Education, enabling secure identity, collaboration, virtual classrooms, research data governance, and e-assessment. Deployment follows the education tenant baseline (identity, SDS, licensing, security) and staged adoption of Teams, SharePoint, and OneDrive with retention schedules and sensitivity labels for research and student records via Microsoft Purview.

TVET scope and specialisations. TVET institutions will be expanded beyond traditional trades to include (i) device and IT maintenance, (ii) campus and community network operations, and (iii) fibre-optic deployment and outside-plant (OSP) works. Curricula will adopt international practice by embedding the Fiber Optic Association (FOA) Certified Fiber Optic Technician (CFOT) baseline and specialist sequences (splicing, testing, OSP, fibre characterisation, FTTx), alongside structured cabling and network-operations modules. These programmes combine classroom learning with hands-on labs in



termination, splicing, OLTS/OTDR testing, safety, and jobsite procedures—precisely the skills industry expects for construction, activation, and maintenance of broadband access.

To ensure work-ready graduates aligned with national connectivity goals, TVET colleges will operate “living labs” on campuses: supervised fibre routes, handholes, cabinets, and Wi-Fi meshes that students install, test, and maintain under faculty and contractor oversight. This design is consistent with FOA’s competency-based approach and allows immediate placement with neutral-host fibre operators and ISPs participating in the open-access model.

Apprenticeship and certification. A co-op placement scheme will pair advanced TVET students with telecom civil-works and ISP partners; FOA proctored examinations will be offered on campus, and specialist credentials (CFOS/S for splicing, CFOS/T for testing, CFOS/O for OSP) will be layered as students progress.

6.3 Primary and Secondary Education (Sequenced Rollout)

Enrolment and classroom operations will be synchronised through SDS so classes, guardians, and timetables flow automatically into Teams for Education. Teachers will use structured lesson channels, assignments, and assessment rubrics; schools will operate in a hybrid model that supports both classroom and remote learning as needed. Microsoft’s admin resources and onboarding paths will guide deployment, while the Ministry’s training arm ensures localisation and support in local languages.

Teacher professional development is anchored in the **UNESCO ICT Competency Framework for Teachers (ICT-CFT)**, Version 3, contextualised to national curriculum. Micro-credentials follow the ICT-CFT’s three progression levels (Technology Literacy, Knowledge Deepening, Knowledge Creation), with in-class coaching and peer-learning communities built into teachers’ workload. This ensures that digital tools translate to better pedagogy, assessment, and inclusion rather than superficial usage.

Inclusive design mandates WCAG 2.1-conformant portals and content, assistive-technology support, and offline-first content packs for schools with intermittent connectivity; link text and navigation will follow WAI guidance for accessible experiences.

6.4 Devices, Device Management, and Labs

Device strategy prioritises **shared, managed devices** in labs and libraries, gradually expanding to 1:1 models where justified by pedagogy and TCO. Devices are enrolled and governed using **Intune for Education** with group-based policies, app deployment, and exam-mode (Take a Test) where needed; profiles enforce encryption, anti-malware, web content filtering, and data loss prevention. This configuration follows Microsoft’s education deployment guidance and ensures safe, compliant operation for minors and staff.

6.5 School Connectivity and Community Benefit

Schools are designated **anchor institutions** in the national open-access broadband plan. Each connected school receives a managed lateral (fibre or high-capacity fixed-wireless) with campus Wi-Fi and a secure edge. This approach mirrors the **Giga** initiative’s global practice—**map** schools, **model** infrastructure and finance, then **contract** affordable connectivity—and uses schools to catalyse connectivity in surrounding communities.

Where fibre build-out lags, satellite or fixed-wireless backstops are applied, with progressive migration to fibre as routes are completed by TVET apprentices and contractors. Performance SLAs and

price/performance baskets are published, and schools' connections are monitored for uptime and throughput, consistent with Giga's real-time mapping ethos.

6.6 Safety, Privacy, and Data Governance in Education

All educational platforms and processes operate under a comprehensive learner-data protection regime: clear roles for controller/processor, records of processing, purpose limitation, minimisation, and data-subject rights—with special safeguards for minors. UNESCO's *Minding the Data* guidance and UNICEF's Data Protection in Schools serve as normative references for policy, DPIAs, parental consent where appropriate, cross-border transfer controls, and vendor terms.

Online safety policies integrate UNICEF and ITU Child Online Protection frameworks, including age-appropriate design, safety-by-default configurations, reporting and response paths, and educator/guardian training. Portals and content conform to WCAG 2.1 and implement clear, descriptive links and navigation to support all learners.

6.7 Platforms, Content, and Assessment

Learning content is curated to national curriculum and reviewed for accessibility, licensing, and pedagogical alignment. **Teams for Education** provides assignments, feedback, and Education Insights, while **Microsoft 365 Education** underpins collaboration and records. Information protection and retention policies (via **Microsoft Purview**) are mandatory for student records, assessments, and research, ensuring encryption, labelling, and auditable access.

Content selection prioritises **open educational resources (OER)** and low-bandwidth formats; where adaptive learning tools are used, procurement mandates transparent algorithms and opt-out choices, consistent with OECD and UNESCO calls for trustworthy data governance in education.

6.8 Monitoring, Evaluation, and Learning (MEL)

The MEL framework tracks access, usage, quality, and learning outcomes with **sex/age/disability/rural-urban** disaggregation. Indicators include: (i) connected universities/TVETs and schools; (ii) active usage of Teams/assignments; (iii) teacher micro-credential completion (ICT-CFT levels); (iv) content accessibility compliance rates; (v) TVET certification outputs (CFOT and CFOS specialist counts); and (vi) foundational learning and progression metrics. Evidence synthesis and course corrections are informed by the **EdTech Hub** library and World Bank EdTech knowledge base.

7. Open-Access Community Broadband (Swedish Model Inspired)

This Chapter establishes the policy, technical, and financing arrangements for a neutral-host, open-access broadband programme designed to accelerate universal, affordable connectivity while preserving national sovereignty over strategic infrastructure. The model is inspired by Sweden's municipally anchored, competition-neutral fibre deployments (e.g., Stockholm's Stokab) and adapted to the realities of South Sudan. It assigns the **passive layer**—ducts and dark fibre—to a public custodian, and invites multiple providers to compete at the **active and retail layers**, thereby expanding choice, lowering prices, and creating local opportunities for service innovation. Evidence from Sweden shows that such open-access models catalysed near-universal FTTP coverage, vibrant service competition, and innovation spill-overs when the infrastructure remained neutral and non-discriminatory.

7.1 Policy Model and Rationale

The policy adopts a **three-layer** structure: (i) publicly owned passive infrastructure (ducts, chambers, building risers, and dark fibre), (ii) a communications-operator function that lights the fibre and offers

wholesale products on equal terms, and (iii) competing retail ISPs that package services for end users. Sweden’s experience—combining municipal neutral-host fibre, a dedicated communications-operator layer, and open retail access—demonstrates that this division of roles lowers barriers to entry, intensifies competition, and sustains long-run efficiency.

South Sudan’s current affordability and adoption constraints justify an open-access approach coupled with **temporary affordability measures**. Internet penetration was estimated at roughly **7%** in early 2023, implying limited demand at full-cost tariffs and reinforcing the need for staged pricing and demand stimulation alongside supply-side investment.

The World Bank’s digital infrastructure guidance further supports policies that **promote effective telecommunications markets** and deploy innovative financing instruments (gap funding, risk-mitigation) to expand coverage and reduce prices in low-income contexts.

In alignment with the Swedish policy ecosystem, the programme will institutionalise mapping and dig-safety coordination practices analogous to **Bredbandskartan** and **Ledningskollen**, which Sweden uses to show coverage, identify owners/operators, and minimise accidental damage during civil works.

7.2 Building-Level Fibre and the Neutral-Host Network

The access network will be built **to and within buildings** (multi-dwelling units, compounds, and public facilities) using a point-to-point dark-fibre topology where practical, with fibre risers, termination panels, and demarcation points provisioned for **non-discriminatory wholesale access**. This approach mirrors Stockholm’s neutral fibre blueprint, which maintains public control of the passive layer and enables operators to deploy their active equipment or lease capacity under transparent conditions.

To ensure long-term resilience and innovation readiness, design standards will provide sufficient ducts and handholes for future overbuilds, 5G small-cell backhaul, and campus interconnection—features identified as success factors in Stockholm’s evolution from dark-fibre availability to a platform for advanced services (e.g., media delivery, health, and even quantum communication pilots).

Custody and ownership. In keeping with the public-infrastructure tradition of open networks, **SUDESA will act as the asset custodian for the passive network**—holding the ducts and fibre as a strategic public asset and conceding wholesale access on equal terms. This arrangement is stated plainly in asset registers and access reference offers, yet operationally subtle in market posture: the programme **encourages licensed ISPs and communications-operator partners to “sell over the fibre”**, rather than crowding out retail or active-layer entrepreneurship. The Swedish municipal precedent of publicly managed passive infrastructure combined with private-sector operations provides a clear reference for this balance.

7.3 Wholesale Access, ISP Marketplace, and Competition

Wholesale access will be organised through a **transparent marketplace** offering a standard product catalogue (dark fibre pairs, lit capacity in stepped bandwidth tiers, VLANs, and managed NNI handoffs), with **non-discriminatory terms, SLAs, and price lists** published and periodically reviewed by the regulator. Sweden’s open-access practice shows that separating passive ownership from active operations and retail **expands provider choice** and avoids vertically integrated bottlenecks; it also facilitates consolidation of operations over time without compromising open access.

A technical **communications-operator (CO)** will manage active equipment and service provisioning to multiple ISPs, aligning with the Swedish three-layer model. ISPs will be onboarded through standard interconnect and service-qualification processes; quality metrics (latency, packet loss, availability) will

be monitored centrally and published to sustain competition on performance and price. Evidence from Stockholm's Stokab and subsequent evaluations underscores that **wholesale-only neutrality** spurs innovation and third-party service diversity when coupled with strict non-discrimination.

7.4 Rights-of-Way, Building Codes, and Wayleave Framework

Rights-of-way (RoW) will be codified in a Dig Once & Coordinate framework, with standard timelines, fees, and trench-sharing incentives. The programme will establish a national underground-plant coordination portal (functionally similar to Sweden's Ledningskollen) to reduce accidental damage, coordinate projects, and enable "one-call" notifications prior to excavation.

Building codes will require fibre-ready risers and internal conduits in new construction and major renovations; utility corridors and micro-trenching will be permitted under uniform specifications. To promote transparency and investor confidence, a public broadband map (akin to Sweden's Bredbandskartan) will display coverage, planned builds, and wholesale availability by location, supporting demand aggregation and informed market entry.

7.5 Universal Service, Affordability, and Last-Mile Options

Given low starting adoption and income constraints, the programme will operate an Affordability Period during which entry-level wholesale products and retail offers are subsidised or price-capped to stimulate uptake, with clear glide-paths to cost-reflective tariffs as utilisation and incomes rise. This design is consistent with World Bank guidance to pair market-enabling regulation with gap financing and risk-mitigation to expand broadband access where private investment alone is unlikely to deliver equitable outcomes.

Blended finance and Nordic participation. To carry early-stage costs, the facility will court Nordic development-finance investors with explicit mandates in digital infrastructure. Finnfund invests in backhaul fibre, towers, data centres, and "connecting the unconnected," and has co-financed African fibre platforms in partnership with peer DFIs and global technology partners—demonstrating both risk appetite and thematic alignment. Swedfund operates under a sustainable-development mandate and has publicly prioritised infrastructure (including digital connectivity) in emerging markets through policies and recent commitments. These institutions can anchor concessional or patient capital that underwrites the Affordability Period and de-risks early deployment.

Technology mix for last mile. While fibre-to-premises is the long-term standard, the programme will pragmatically integrate **fixed-wireless** for rapid expansion where densities or terrains render fibre uneconomic in the near term, migrating to fibre as demand matures. This is consistent with international practice prioritising coverage, competition, and affordability over strict technology orthodoxy.

7.6 Satellite and Resilience for Remote Areas

For sparsely populated and hard-to-reach localities, and for fail-over resilience, the network will integrate satellite backhaul (including LEO where available) with policy-based routing to critical sites such as clinics, schools, and administrative offices. The resilience architecture will include multi-route backhaul, diverse power options, and service-class differentiation to keep essential services online during terrestrial disruptions. Global connectivity briefs emphasise that reliable and affordable internet—delivered through a mix of terrestrial and non-terrestrial means—underpins participation in modern society and service delivery, particularly in remote areas.



Pricing, Subsidy, and Thresholds: How the Affordability Period Works

During Years 1–3, wholesale and entry-level retail tariffs are temporarily reduced through a pre-agreed subsidy envelope funded by SUDESA's broadband facility and Nordic co-investors, with revenue-sharing triggers and utilisation thresholds (e.g., take-up per node, average bandwidth consumption) that phase tariffs toward cost-reflective levels as the market deepens. This approach avoids permanent distortions, supports market discovery, and maintains transparent terms for all ISPs. The mechanism is compatible with the World Bank's recommended gap-funding and risk-sharing instruments for early-stage broadband markets.

Governance, Transparency, and Investor Protections

Procurement of civil works, fibre, active equipment, and managed services will be published end-to-end in **Open Contracting Data Standard (OCDS)** to ensure full transparency and competitive neutrality. Environmental and social screening and instruments will follow the **World Bank ESF** and **AfDB ISS**—including community health and safety during excavation, labour standards, and grievance redress—thereby aligning the programme with international safeguards expected by responsible investors.

Outcome: A Neutral, Publicly Owned Spine with Vibrant Private Competition

In sum, the **passive network remains a public, neutral platform**—with SUDESA as its custodian—while the **active and retail layers are opened to competition**, inviting licensed ISPs to build brands, bundle services, and win customers on price and quality. The Swedish record shows that such a model is **compatible with scale, innovation, and long-term efficiency** when governance, access conditions, and planning tools are robust; the financing plan adds a needed affordability bridge for South Sudan's present market conditions.

Principal sources and further reading: Sweden's municipal open-access history and three-layer model

[Analysys Mason](#)

[WIK-Consult 2023](#)

[Stokab reports page](#)

[EC overview](#)

[Ledningskollen](#)

[World Bank digital infrastructure brief](#)

[Connectivity & Networks](#)

[DataReportal 2023](#)

[Finnfund sector note](#)

[DFC–Finnfund–Google investment note](#)

[Swedfund guidelines and connectivity focus](#)

8. Compliance, Data Protection, and Cybersecurity

This Chapter codifies the legal, organisational, and technical safeguards that render the digital state trustworthy, auditable, and resilient. It integrates a rights-based Data Protection and Privacy Framework, a risk-driven cybersecurity programme aligned to NIST CSF 2.0 and ISO/IEC 27001:2022,



and a CERT/SOC operating model for incident readiness and response. Records and evidence are governed under recognised records-management standards with enterprise-grade audit trails. These regimes are harmonised with continental and donor norms—most notably the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and multilateral safeguards expectations—so that citizens’ rights, institutional legitimacy, and investor confidence reinforce each other.

8.1 Data Protection and Privacy Framework (DPIA Regime)

Legal basis and scope. South Sudan’s Data Protection and Privacy Act will be drafted and implemented to reflect the Malabo Convention’s substantive guarantees—lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, and accountability—together with rules for cross-border transfers based on **adequate protection** or appropriate safeguards and regulatory oversight. Supervisory authority powers, notification/registration obligations, and sanctioning regimes are defined in statute and regulations so that oversight is effective, independent, and accessible.

DPIA regime. Any processing “likely to result in a high risk” to individuals’ rights—e.g., large-scale use of sensitive data, systematic monitoring, or innovative technologies—requires a documented **Data Protection Impact Assessment (DPIA)** before go-live, with mitigation measures embedded in design and contracts. Methodology and thresholds follow **EDPB/Article 29** guidance (WP248 rev.01), with local adaptations issued by the supervisory authority; practical templates and checklists follow established supervisory practice (e.g., ICO) and are integrated into the DTSC stage-gates.

Identity and inclusion safeguards. Foundational and functional ID systems are governed by **ID4D Principles** on inclusion, technology neutrality, privacy by design, and independent oversight (e.g., redress and grievance). Consent, transparency, and purpose limitation are enforceable at the API layer, with auditable logs of disclosures; legitimate-interest balancing tests, children’s data protections, and special-category rules are codified in regulations.

Cross-regime consistency and remedies. Public disclosure obligations (e.g., procurement and performance transparency) remain subject to lawful, narrowly tailored redactions for privacy, national security, and commercial confidentiality, with decisions documented and appealable. Stakeholder engagement and grievance redress are operated in accordance with multilateral safeguards practice for public projects.

8.2 Cybersecurity Framework (ISO/IEC 27001:2022; NIST CSF 2.0)

Cybersecurity governance will combine the NIST Cybersecurity Framework (CSF) 2.0 for outcome-oriented risk management with a certifiable Information Security Management System (ISMS) under ISO/IEC 27001:2022. The NIST CSF supplies a common taxonomy and governance structure—Govern–Identify–Protect–Detect–Respond–Recover—used to set ministry-level Profiles, targets, and metrics, while ISO/IEC 27001 provides the management-system engine for risk assessment, control selection, competence, documentation, internal audit, and continual improvement. This twin-track model enables clear executive oversight and measurable assurance while allowing proportionate, context-specific controls in each entity.

Sources: **NIST CSF 2.0** (core document and governance constructs) — nist.gov/cyberframework and CSWP 2.0 — nvlpubs.nist.gov; **ISO/IEC 27001:2022** (ISMS requirements) — iso.org.



Integration between the two frameworks is facilitated by NIST’s OLIR mapping, which links ISO/IEC 27001:2022 controls and practices to CSF 2.0 functions and categories so that ministries can evidence CSF outcomes through their ISMS and vice-versa. Practically, this means a single risk register and Statement of Applicability underpin management decisions, while CSF Profiles express target posture and progress to leadership and partners in a language they recognise. *Sources:* NIST CSF 2.0 site (OLIR informative references, including “ISO/IEC-27001:2022-to-CSF 2.0” mapping posted May 30, 2025) — nist.gov/cyberframework.

From a control perspective, the ISMS will adopt Zero-Trust design as policy and architecture—explicit verification with strong, contextual authentication; least-privilege access (including just-in-time and just-enough administration); and an assumed-breach mindset with segmentation, encryption, and continuous monitoring. The operational deployment sequence follows Microsoft’s and NIST’s implementation guidance across the seven technology pillars (identities, endpoints, data, applications, infrastructure, networks, and visibility/automation), ensuring that identity becomes the primary control plane and that telemetry is centrally analysed to reduce dwell time.

Sources: Microsoft Zero Trust Guidance Center (principles and deployment plans) — learn.microsoft.com; Zero Trust deployment overview — learn.microsoft.com.

“Detect” and “Respond” capabilities rely on policy-driven logging and monitoring of identity, endpoint, network, application, and cloud control-plane events, with retention and integrity safeguards aligned to NIST SP 800-92 guidance on log management. Incident readiness and lifecycle management (prepare–detect/analyse–contain/eradicate/recover–lessons learned) will align to NIST SP 800-61 (latest revision, Rev. 3), ensuring methodological coherence with CSF 2.0 and providing repeatable playbooks for the national CERT and ministry SOC functions.

Sources: NIST SP 800-92 (log management) — csrc.nist.gov and draft revision — nvlpubs.nist.gov; NIST SP 800-61 Rev. 3 (incident response profile with CSF 2.0 alignment) — csrc.nist.gov.

Finally, continuous improvement will be institutionalised through internal audits, management reviews, corrective actions, and—where mandated—third-party ISO/IEC 27001 certification for high-risk entities. Ministries will publish CSF Profile summaries and maturity targets annually to the DTSC, using a common metrics catalogue, while the ISMS provides documentary evidence of control effectiveness. This closed-loop assurance—CSF outcomes expressed to leadership, ISO controls audited for effectiveness—delivers defensible compliance and improves national cyber resilience over time.

Sources: NIST CSF 2.0 (Profiles and Tiers for governance and measurement) — nist.gov/cyberframework; ISO/IEC 27001:2022 (management system audits and continual improvement) — iso.org.

8.3 Government CERT and Incident Response

Mandate and governance. South Sudan will establish a Government Computer Emergency Response Team (Government-CERT) by statutory instrument, mandated to prevent, detect, coordinate, and respond to cybersecurity incidents affecting ministries, state-owned enterprises, and designated critical sectors. The Government-CERT’s service catalogue and maturity model will be defined with reference to the FIRST CSIRT Services Framework, ensuring a clearly scoped portfolio (incident handling, vulnerability management, situational awareness, threat intelligence, advisories) and transparent service levels for its constituency. The framework also provides a common vocabulary and structure for capability development and measurement across the incident-management lifecycle.



Sources: FIRST, CSIRT Services Framework v2.1 (purpose, services and functions) —

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1; FIRST, **v1.1 PDF** (hierarchical model and detailed service descriptions) —

https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v1.1.pdf

Operating model with the national SOC. The Government-CERT will operate in tight coordination with the national SOC. CERT analysts consume telemetry and alerts from the SOC and lead incident command when events cross organisational boundaries or escalate to national significance. Processes, playbooks, and reporting are aligned to NIST SP 800-61 (Rev. 3)—preparation; detection and analysis; containment, eradication, and recovery; and post-incident lessons learned—thereby harmonising day-to-day operations with the NIST Cybersecurity Framework (CSF) 2.0 functions “Detect” and “Respond.” The Rev. 3 update explicitly integrates incident-response recommendations with CSF 2.0 risk management, facilitating consistent governance, metrics, and board-level reporting.

Sources: NIST, SP 800-61 Rev. 3 (CSF-aligned incident response) — <https://csrc.nist.gov/pubs/sp/800/61/r3/final>; NIST, **CSF 2.0** overview and materials — <https://www.nist.gov/cyberframework>.

Establishment guidance and capability building. The programme for standing up the CERT—governance, staffing profiles, technology stack, SLAs, and performance metrics—will follow **ENISA’s guidance on setting up CSIRTs and SOCs**, adapted to the national context. This includes structuring services and interfaces, selecting tooling, defining escalation paths, and instituting continuous improvement based on exercises and metrics (e.g., mean time to detect/respond).

Sources: ENISA, **How to set up CSIRT and SOC** (good-practice guide) —

<https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc> ENISA, **Good Practice Guide for Incident Management** — <https://enisa.europa.eu/publications/good-practice-guide-for-incident-management>.

Automation and orchestration. To cope with alert volume and accelerate containment, the CERT will operate a SIEM/SOAR workflow that automates enrichment and standard responses under change-controlled playbooks, with manual analyst approval for destructive or high-risk actions. This approach is consistent with current practice in **cloud-native SIEM/SOAR** operations, where automation rules and playbooks reduce analyst load and improve consistency.

Sources: Microsoft, Sentinel automation (SOAR) guidance — <https://learn.microsoft.com/en-us/azure/sentinel/automation/automation>; Microsoft, SIEM/XDR community resources — <https://github.com/Azure/Azure-Sentinel/wiki>.

Notification and legal interface. Breach-notification timelines, thresholds, and content will be defined in secondary legislation consistent with the **Malabo Convention’s** data-protection principles (lawfulness, security of processing, and safeguards for transfers). The CERT will publish public advisories and Indicators of Compromise, and will participate in regional and international information-sharing communities under appropriate traffic-light protocols.

Sources: African Union, **Malabo Convention** (data-protection and security obligations) — <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>; consolidated text (PDF) — <https://dataprotection.org.gh/wp-content/uploads/2025/05/Malabo-Convention.pdf>.



Post-incident learning and assurance. Following each major incident, the CERT leads a root-cause analysis and lessons-learned review, updates playbooks, and recommends risk-remediation plans to the DTSC. This is in line with **NIST SP 800-61 (Rev. 3)** expectations for institutional learning and with the continuous-improvement loop required by **ISO/IEC 27001:2022** (management review and corrective action).

Sources: NIST, **SP 800-61 Rev. 3** (post-incident activity) —

<https://csrc.nist.gov/pubs/sp/800/61/r3/final> ISO, **ISO/IEC 27001:2022** (ISMS—continual improvement) — <https://www.iso.org/standard/27001> .

8.4 Information Governance, Records, and Audit Trails

Records policy and standards. Government records—whether born-digital or digitised—will be governed by a formal records-management policy grounded in **ISO 15489-1:2016** (concepts and principles for records management) and the functional requirements for managing digital records set out in **ISO 16175-1:2020**. Together, these standards require that records (and their metadata) be created, captured, classified, retained, and disposed of in a manner that preserves their authenticity, reliability, integrity, and usability over time—irrespective of format or system of origin.

Sources: ISO, **ISO 15489-1:2016** (records management principles) —

<https://www.iso.org/standard/62542.html> ISO, **ISO 16175-1:2020** (functional requirements for software managing digital records) — <https://www.iso.org/standard/74294.html>

Audit trails and digital evidence. Security-relevant and legally significant events (access, administrative actions, configuration changes, data exports, API calls, and workflow decisions) must be recorded in **immutable, time-stamped audit trails** with clock synchronisation and integrity safeguards. Log-management policies will adopt **NIST SP 800-92** guidance for establishing enterprise logging, normalisation, retention, and protection, recognising logs as evidentiary records that support investigations and audits. Retention schedules will balance investigative value with privacy and storage constraints, and integrity protections (e.g., hash chaining, WORM storage, or trusted archival services) will be applied proportionately to risk.

Sources: NIST, **SP 800-92** (Guide to Computer Security Log Management) —

<https://csrc.nist.gov/pubs/sp/800/92/final>; NIST, **SP 800-92r1 (initial public draft)** (updated cybersecurity log-management guidance) — <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-92r1.ipd.pdf>.

Discovery, holds, and accountability. The State will maintain enterprise eDiscovery and audit capabilities to place legal holds, search across repositories, review, export, and log every administrative action taken by investigators or case managers. For Microsoft-based estates, Microsoft Purview provides auditable trails of eDiscovery activities and role-based access enforcement; equivalent capabilities will be required of any alternative platform through procurement specifications.

Sources: Microsoft, Search for eDiscovery activities in the audit log (Purview) —

<https://learn.microsoft.com/en-us/purview/edisc-ref-audit-log>; Microsoft, Audit search — <https://learn.microsoft.com/en-us/purview/audit-search>.

Public contracting and programme transparency. To ensure probity and enable external scrutiny without compromising personal data, all procurement data and documents will be disclosed end-to-end (planning, tender, award, contract, implementation) using the Open Contracting Data

Standard (OCDS), while applying lawful, narrowly tailored redactions for privacy, security, or commercial sensitivity. This approach aligns transparency with privacy law and is consistent with multilateral safeguards' disclosure and grievance principles.

Sources: Open Contracting Partnership, **OCDS documentation** — <https://standard.open-contracting.org/latest/en/>; World Bank, **Environmental and Social Framework** (disclosure and stakeholder engagement norms) — <https://www.worldbank.org/en/projects-operations/environmental-and-social-framework>.

Safeguards coherence and appeals. Records of stakeholder engagement, grievances, and incident notifications will be maintained and disclosed according to safeguards policies, enabling traceable remedies and oversight. For AfDB-supported activities, the updated Integrated Safeguards System (ISS), effective 31 May 2024, governs environmental and social requirements, including community health and safety and stakeholder engagement in higher-risk operations.

Sources: AfDB, ISS update becomes effective (press release, 4 Jun 2024) — <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>; World Bank, ESF — <https://www.worldbank.org/en/projects-operations/environmental-and-social-framework>.

Outcome. By professionalising incident response under a Government-CERT aligned to international CSIRT practice and by institutionalising records governance and auditability under ISO standards and NIST guidance, South Sudan will achieve verifiable accountability, defensible evidence handling, and resilient response. This framework satisfies regional legal norms (**Malabo**), international security governance (**CSF 2.0/ISO 27001**), and donor safeguards (ESF/ISS), thereby strengthening citizen trust and investor confidence.

Sources: African Union, **Malabo Convention** — <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>; NIST, **CSF 2.0** — <https://www.nist.gov/cyberframework>; ISO, **ISO/IEC 27001:2022** — <https://www.iso.org/standard/27001>.

9. Procurement, Open Contracting, and Vendor Neutrality

9.1 Procurement Policy and Procedures

SUDESA will operate a rules-based, competition-neutral procurement regime that is fully aligned with the World Bank Procurement Regulations for IPF Borrowers and their core principles—value for money, economy, integrity, fit-for-purpose, efficiency, transparency, and fairness—thereby ensuring donor eligibility, market confidence, and consistent redress mechanisms. The Seventh Edition (September 2025) will be adopted as the authoritative reference, complemented by the Bank's Standard Procurement Documents (SPDs) and Borrower guidance for operational clarity and training. This framework permits tailoring of approaches-to-market (e.g., Request for Bids, Request for Proposals), use of rated criteria, and determination of the Most Advantageous Bid, while preserving equal treatment and non-discrimination. Procurement planning, prior/post review thresholds, and contract management shall be governed by a written manual cross-referencing these instruments.

Sources: World Bank, Procurement Regulations for IPF Borrowers (Seventh Ed., Sep 2025) — <https://thedocs.worldbank.org/en/doc/c84273d1b230aeb2b0b8134de5dc8cd7-0290012025/original/Procurement-Regulations-7th-Edition-Sep-2025.pdf>



World Bank, Beginner's Guide for Borrowers (Nov 2023)

<https://thedocs.worldbank.org/en/doc/caf6a3f677305292d799dbe55fd83bfe-0290012023/original/PROCUREMENT-Beginners-Guide-to-IPF-WEB-VERSION-Nov-2023.pdf>

World Bank, SPDs overview

<https://documents1.worldbank.org/curated/en/099050124135714137/pdf/P166640169f11c0c1baab182813c9e4073.pdf>

Procedural due process will include a standstill/notification window (as applicable under the selected SPD) and a documented complaints-handling process with time-bound acknowledgements, reasons for decision, and escalation/record-keeping, consistent with World Bank guidance. Implementing agencies shall disclose Contract Award Notices and maintain a register of procurement-related complaints and resolutions available for audit and public inspection in accordance with access-to-information rules.

Sources: World Bank, Guidance: Procurement-related Complaints (Annex III reference)

<https://thedocs.worldbank.org/en/doc/975671478891365829-0290022017/original/GuidanceProcurementrelatedComplaints.pdf>

World Bank, Complaints – how to file

<https://thedocs.worldbank.org/en/doc/6b32629dd1e7e1f60ae23a3daeec2b6a-0290012025/original/Procurement-complaints-filing.pdf>

Sanctions screening is mandatory. Bidders, contractors, and key principals shall be checked against the World Bank Listing of Ineligible Firms and Individuals; cross-debarment under the April 2010 MDB agreement applies, and any ineligibility will trigger rejection or contract action in line with the Regulations. SUDESA will retain screening evidence in the contract file.

Sources: World Bank, Debarred & Cross-Debarred List — <https://www.worldbank.org/en/projects-operations/procurement/debarred-firms> (cross-debarment noted)

9.2 Open Contracting Data Standard (OCDS) Publication

All procurement data and documents will be published end-to-end—planning, tender, award, contract, and implementation—using the **Open Contracting Data Standard (OCDS)**, ensuring machine-readability, comparability, and public scrutiny while enabling internal analytics and donor reporting. The publication pipeline will be integrated with SUDESA's e-Procurement platform and the disclosure portal; release and record packages will be validated with the official **OCDS Data Review Tool** before publication, and data-quality dashboards will be disclosed alongside the datasets.

Sources: Open Contracting Partnership, **OCDS documentation (latest)** — <https://standard.open-contracting.org/latest/en/>

OCDS Data Review Tool (validator) — <https://review.standard.open-contracting.org/>

For infrastructure-heavy components (e.g., backbone, metro fibre, campus builds), SUDESA will publish **project-level** disclosure in the **Open Contracting for Infrastructure Data Standard (OC4IDS)** to connect project preparation, risk registers, contract changes, and delivery milestones to the underlying contracting releases, thereby improving whole-life transparency and performance management. Implementation guidance (project identifiers, packaging models, and integration with procurement systems) will be followed.

Sources: OCP/CoST, **OC4IDS Toolkit** — <https://standard.open-contracting.org/infrastructure/latest/en/>



OC4IDS overview — <https://infrastructuretransparency.org/resource/oc4ids-a-new-standard-for-infrastructure-transparency/>

OC4IDS implementation guidance

<https://standard.open-contracting.org/infrastructure/latest/en/guidance/>

Where beneficial ownership (BO) is collected or linked, contracting data will reference a separate BO register conformant with the Beneficial Ownership Data Standard (BODS), using consistent organisation identifiers to join data for risk-screening and public scrutiny; where a separate register is not yet available, OCDS' BO extension can be used with clear provenance and update rules. Sources: Open Contracting, Beneficial ownership in OCDS (mapping & options) — https://standard.open-contracting.org/latest/en/guidance/map/beneficial_ownership/

Open Ownership, **BODS (documentation)** — <https://standard.openownership.org/>

9.3 Competition, Beneficial Ownership, and Complaints Handling

To enlarge contestability and prevent market foreclosure, SUDESA will apply non-discriminatory qualification, proportionate technical requirements, and transparent, pre-published evaluation criteria that award on **Most Advantageous Bid** (price and quality) rather than lowest price alone. The Regulations permit rated criteria and negotiation where appropriate; these tools will be used judiciously to deliver value for money while safeguarding fairness and integrity. A register of procurement decisions will document the rationale for chosen approaches-to-market, evaluation results, and contract awards.

Source: World Bank, **Beginner's Guide for Borrowers (evaluation, Most Advantageous Bid, rated criteria)** — <https://thedocs.worldbank.org/en/doc/caf6a3f677305292d799dbe55fd83bfe-0290012023/original/PROCUREMENT-Beginners-Guide-to-IPF-WEB-VERSION-Nov-2023.pdf>

Beneficial ownership transparency is an integral anti-corruption safeguard: winners above set thresholds

References: OECD Recommendation and implementation reports ([OECD 2015/2025](#) [2020–2024 review](#))

UNCITRAL Model Law (chapters on participation, descriptions, evaluation criteria) ([UN 2011/2014 ed.](#)

World Bank Procurement Regulations (4th ed., Nov 2020) ([PDF](#))

To prevent conflicts of interest, collusion through related-party bidding, and concealed debarments, the system mandates **beneficial-ownership (BO) disclosure** for all tenderers and key subcontractors as a condition of participation, with legally binding declarations at submission, award and contract-change stages. Data will be collected and published using the **Beneficial Ownership Data Standard (BODS)** and linked at tender and award stages through the **Open Contracting Data Standard (OCDS)** identifiers, enabling automated red-flagging and public oversight. International guidance recognises BO integration with procurement as a proven measure to deter fraud, fortify integrity screening, and improve competitive outcomes.

References: **Open Ownership – BODS** ([standard site](#) [OO overview](#))

Open Contracting Partnership (beneficial ownership in procurement) [policy note](#) [overview page](#)

OCDS documentation [data model](#)

A **time-bound, independent complaints system** will be operated for procurement challenges. It will include: (i) acknowledgment and decision deadlines; (ii) access to debriefing; (iii) a standstill period before contract signature to allow effective review; (iv) an impartial review body with powers to recommend suspension or corrective action; and (v) publication of outcomes with reasoning, subject to lawful redactions. This approach is consistent with UNCITRAL's model remedies for supplier challenges and the World Bank Procurement Regulations requirements on complaints handling, debriefing and standstill practices in IPF operations. For projects financed by other MDBs, the respective rules on bidder review and grievance redress will apply in parallel. *References:* **UNCITRAL Model Law** (supplier remedies framework) [text](#)

World Bank Regulations ([Nov 2020](#))

All complaints, BO declarations, exclusion decisions and conflict-of-interest determinations will be digitally logged and published through the national open-contracting portal, linked to the procurement's ocid. This ensures a verifiable chain of decisions for auditors and the public, in line with international best practice on transparency and accountability in public procurement. *References:* OCDS documentation [publication guidance](#)

OECD on transparency and competition across the procurement cycle [overview](#)

9.4 Anti-Lock-In Measures and Open Standards

To preserve vendor neutrality and ensure long-term interoperability, every procurement under the SUDESA framework will incorporate explicit anti-lock-in provisions covering data, interfaces, identity, and infrastructure. These provisions are not optional—they are embedded as mandatory contractual clauses and enforced through stage-gate reviews and acceptance testing.

Core Requirements:

1. **Comprehensive Exit Plans and Data Portability from Day One**

Each supplier must deliver a documented **exit strategy** at contract inception, detailing timelines, responsibilities, and technical procedures for full disengagement without service disruption. This includes **data export rights in open, machine-readable formats** (e.g., XML, JSON, CSV) and the ability to re-host workloads on alternative platforms without proprietary dependencies.

2. **Ownership and Escrow of Configuration Artefacts and Documentation**

All configuration scripts, deployment templates, and system documentation are classified as **deliverables owned by the contracting authority**. Where proprietary components are unavoidable, **source code or configuration escrow** arrangements will be established to guarantee continuity in the event of vendor default or termination.

3. **Publication of Open, Documented APIs**

Systems must expose **publicly documented APIs** for all core functions, enabling integration with third-party applications and future platforms. API specifications must follow open standards (e.g., REST/JSON, OpenAPI) and be versioned with backward compatibility guarantees.

4. **Use of Open Standards for Data and Document Formats**

All persistent data and official documents must comply with **open, internationally recognised standards** (e.g., ISO/IEC 26300 for ODF, ISO 19005 for PDF/A, ISO 8601 for date/time, UTF-8 for

character encoding). This ensures that records remain accessible and portable across systems and jurisdictions.

Policy Basis and International Guidance:

This approach follows the European Commission’s guidance “Against lock-in: building open ICT systems” (COM(2013) 455 final), which instructs public buyers to specify standards that guarantee interoperability and portability, and to avoid brand-specific dependencies that undermine competition and inflate lifecycle costs. The guidance emphasises that open standards and exit strategies are essential to maintain competitive tension, reduce switching costs, and protect public investment over time.

References:

- European Commission, “Against lock-in: building open ICT systems” — EUR-Lex COM(2013) 455 final;
- Official PDF — ec.europa.eu.

Enforcement and Assurance:

- **Contractual Clauses:** Anti-lock-in obligations are embedded in the General Conditions of Contract and reinforced by specific technical schedules.
- **Stage-Gate Verification:** DTSC will not clear Gate 3 (Go-Live) unless exit plans, API documentation, and open-format compliance are evidenced.
- **Performance Audits:** Annual compliance audits will verify adherence to open-standards commitments and portability guarantees, with penalties for non-conformance.
- **Transparency:** All API specifications and open-standard mappings will be published on the Government’s developer portal, ensuring equal access for all market participants.

10. Financing Architecture and Fiduciary Controls

This chapter defines the financial governance model that underpins the Mission, ensuring predictable funding flows, robust fiduciary safeguards, and compliance with international standards. The architecture is designed to attract blended finance from development partners and private investors while maintaining transparency, accountability, and cost efficiency.

10.1 Digital Transformation Investment Facility (DTIF)

The DTIF is the dedicated financing vehicle for all digitalisation and broadband initiatives under SUDESA. It operates as a ring-fenced fund with its own charter, governance structure, and fiduciary controls, approved by the Joint Steering Committee (JSC). The DTIF’s objectives are:

- **Pooling of Resources:** Aggregate contributions from government, development partners, Nordic DFIs (e.g., Finnfund, Swedfund), and private co-investors into a single, rules-based facility.
- **Predictable Disbursement:** Ensure timely funding for multi-year programmes, avoiding fragmentation and cash-flow volatility.
- **Risk Mitigation:** Apply structured instruments (guarantees, gap funding, viability gap subsidies) to de-risk early-stage investments in broadband and digital infrastructure.



- **Transparency and Assurance:** Operate under IPSAS-compliant accounting, independent audits, and open contracting disclosure.

The DTIF governance includes:

- **Facility Board:** A sub-committee of the JSC with fiduciary oversight.
- **Independent Audit Committee:** Ensures external audit independence and reports directly to the JSC.
- **Disclosure Policy:** All financial statements, procurement data, and performance reports are published in machine-readable formats, subject to lawful redactions.

10.2 IPSAS-Compliant Financial Management

The DTIF adopts the **International Public Sector Accounting Standards (IPSAS)** for recognition, measurement, and disclosure of financial transactions. This ensures comparability, transparency, and donor confidence. Key features include:

- **Accrual-Based Accounting:** Recognition of assets, liabilities, revenues, and expenses when they occur, not when cash changes hands.
- **Chart of Accounts Harmonisation:** Align with national PFM systems while maintaining facility-specific coding for donor reporting.
- **Internal Control Framework:** Based on **COSO** principles, covering control environment, risk assessment, control activities, information and communication, and monitoring.
- **Internal Audit Function:** Operating under **IIA Standards**, reporting to the Audit & Risk Subcommittee of the JSC.
- **External Audit:** Annual audits by an independent, internationally recognised firm, with reports disclosed publicly.

10.3 Disbursement, Treasury, and Cost Recovery Policy

Disbursement Modalities:

- **Direct Payment:** For large contracts (e.g., infrastructure, software licences) to suppliers upon verified milestones.
- **Reimbursement:** For eligible expenditures incurred by implementing entities, subject to prior approval.
- **Advances:** Limited to defined ceilings, backed by bank guarantees or equivalent instruments.

Treasury Management:

- **Segregated Bank Accounts:** Dedicated accounts for DTIF funds, reconciled monthly.
- **Dual Authorisation:** All payments require two authorised signatories, with system-enforced controls.
- **Investment Policy:** Idle funds invested in low-risk instruments (e.g., government securities) to preserve capital and liquidity.

Cost Recovery:

- **Administrative Fee:** A transparent percentage applied to donor contributions to cover facility overheads.
- **Service Charges:** For optional value-added services (e.g., technical assistance) provided to private partners.
- **Glide Path to Sustainability:** Over 10 years, broadband wholesale revenues and cost-sharing arrangements will progressively offset operational costs.

10.4 Partner Contributions and Co-Financing Modalities

The financing strategy blends **public, concessional, and private capital**:

- **Government Contribution:** Budgetary allocation for core operations and legal reforms.
- **Development Partners:** Grants and concessional loans from multilateral banks (World Bank, AfDB) and bilateral donors.
- **Nordic DFIs:** Finnfund and Swedfund as anchor investors in broadband infrastructure, leveraging their mandates for sustainable development and digital inclusion.
- **Private Sector:** Equity and debt participation in active-layer operations and ISP marketplace, under open-access principles.
- **Performance-Based Triggers:** Disbursement linked to compliance milestones (OCDS publication, ESF/ISS safeguards) and KPI achievement (coverage, affordability, service quality).

Transparency and Reporting:

All contributions, commitments, and disbursements are disclosed quarterly on the DTIF portal, tagged with **OCDS identifiers** for traceability. Annual financial statements and performance reports are published in open formats, reinforcing accountability and investor confidence.

11. ESG Safeguards and Human Rights

This chapter sets out the environmental, social, and governance (ESG) safeguards that govern all activities under the SUDESA Mission. These safeguards are not ancillary—they are binding obligations embedded in legal instruments, procurement documents, and operational manuals. They ensure that digital transformation advances human dignity, environmental stewardship, and social inclusion, while meeting the compliance expectations of development partners and private investors.

11.1 Environmental and Social Frameworks (WB ESF; AfDB ISS)

All projects financed through the DTIF will comply with the World Bank Environmental and Social Framework (ESF) and the African Development Bank's Integrated Safeguards System (ISS), updated and effective as of 31 May 2024. These frameworks provide the normative baseline for risk classification, mitigation, and monitoring across ten Environmental and Social Standards (ESS) under ESF and the AfDB's five operational safeguards.

Key obligations include:

- **Environmental and Social Screening:** Every activity undergoes risk classification (Low, Moderate, Substantial, High) before procurement. Screening outcomes and instruments (ESMP, LMP, SEP, RAP) are disclosed on the SUDESA portal.



- **Stakeholder Engagement and Disclosure:** A Stakeholder Engagement Plan (SEP) is mandatory for all substantial-risk activities, ensuring meaningful consultation and accessible grievance mechanisms.
- **Labour and Working Conditions:** Compliance with ESS2 and AfDB OS5, including prohibition of child and forced labour, occupational health and safety measures, and worker grievance channels.
- **Community Health and Safety:** Risk assessments for civil works (e.g., trenching for fibre) and mitigation measures (traffic management, signage, PPE for workers and communities).
- **Biodiversity and Cultural Heritage:** Routing of fibre and siting of facilities must avoid critical habitats and respect cultural heritage, with chance-find procedures in place.

References:

- World Bank, **Environmental and Social Framework** — [worldbank.org](https://www.worldbank.org)
- AfDB, **Integrated Safeguards System (ISS) Update** — [afdb.org](https://www.afdb.org)

11.2 SEA/SH Prevention and Response

The Mission adopts a zero-tolerance policy for Sexual Exploitation and Abuse/Sexual Harassment (SEA/SH). This is operationalised through:

- **Codes of Conduct:** Mandatory for all contractors and staff, with explicit SEA/SH prohibitions and sanctions.
- **Survivor-Centred Response:** Confidential reporting channels, referral pathways to health and psychosocial services, and protection against retaliation.
- **Contractual Remedies:** SEA/SH clauses in all contracts, enabling suspension or termination for non-compliance.
- **Monitoring and Disclosure:** SEA/SH incident statistics (anonymised) reported quarterly to the JSC and disclosed in aggregate on the public dashboard.

These measures align with World Bank Good Practice Note on SEA/SH and AfDB's gender and social safeguards requirements.

11.3 Community Health, Safety, and Grievance Redress

Community Health and Safety:

Civil works for broadband deployment (e.g., trenching, pole erection) will follow strict safety protocols: traffic management plans, signage, PPE for workers, and community awareness campaigns. Emergency preparedness plans will be in place for high-risk sites.

Grievance Redress Mechanism (GRM):

A multi-tier GRM will be established:

- **Tier 1:** Local-level complaint desks and hotline.
- **Tier 2:** SUDESA Safeguards Unit review.
- **Tier 3:** Independent Appeals Panel for unresolved cases. All grievances are logged, tracked, and disclosed in anonymised form, with resolution timelines monitored by the MELR Department.

11.4 E-Waste, Energy, and Green Data Centres

Digitalisation generates environmental externalities—particularly **e-waste** and **energy consumption**. The Mission addresses these through:

- **E-Waste Management:** Contracts for device supply include take-back obligations and certified recycling in compliance with **Basel Convention** principles.
- **Energy Efficiency:** Data centres and SOC facilities will adopt **ISO 50001 Energy Management** standards and target **PUE (Power Usage Effectiveness) ≤ 1.5** .
- **Renewable Integration:** Progressive integration of solar and hybrid systems for data centres and network nodes, reducing reliance on diesel generators.
- **Green Procurement:** Preference for devices and equipment meeting **Energy Star** or equivalent certifications.

Outcome:

By embedding ESG safeguards into every stage—from design to decommissioning—the Mission ensures that digital transformation does not compromise environmental integrity, social equity, or human rights. Compliance with **ESF**, **ISS**, and global best practices positions SUDESA as a model for responsible digital development in fragile contexts.

12. Monitoring, Evaluation, and Learning (MEL)

The Monitoring, Evaluation, and Learning (MEL) regime will function as a single, legally anchored system that binds programme finance, safeguards, and delivery into verifiable results over the ten-year horizon. It is designed to measure what matters (governance integrity, education equity, and affordable connectivity), to publish the evidence in forms that external parties can examine, and to adapt course when the facts compel adjustment. The framework draws on the OECD-DAC evaluation criteria—relevance, effectiveness, efficiency, impact, sustainability, and coherence, as revised in 2019—to give evaluations a shared language and to ensure that equity, synergies, and trade-offs are examined transparently rather than assumed away ([OECD DAC, “Evaluation Criteria: Adapted Definitions and Principles for Use,” 2019](#); see also the EvalNet “Better Criteria for Better Evaluation” material that operationalises those definitions for commissioners and evaluators ([OECD/EvalNet overview](#))). Parallel obligations arising from donor safeguards—namely the World Bank Environmental and Social Framework (ESF) and the African Development Bank’s updated Integrated Safeguards System (ISS)—are hard-wired into MEL so that disclosure, stakeholder engagement, and grievance redress are evidenced in the same public record as financials and outputs ([World Bank ESF portal](#); [AfDB ISS, effective 31 May 2024](#)).

Framework and scope. MEL will operate at three temporal levels that are reflected in the Mission’s legal instruments. At the impact level (ten years), it will test whether South Sudan has transitioned to a digitally sovereign administration, an inclusive education system with sustained digital competences, and a competitive broadband market that people can actually afford. At the outcome level (three to six years), it will assess whether ministries have consolidated on enterprise-grade collaboration and identity, whether universities and TVETs are persistently connected and using managed devices and platforms, and whether open-access broadband has reached critical mass in buildings and community nodes. At the output level (annual), it will verify the deployments, trainings, nodes, and services delivered against plan. These tiers are not mere labels; they bind statutory reporting and procurement disclosure so that each financial flow and each contract can be traced to a result through a stable

identifier published in the **Open Contracting Data Standard (OCDS)** pipeline ([OCDS documentation](#); [World Bank OCDS brief](#)).

Baselines and measurement. The first task of MEL is to establish credible baselines, recognising that current internet use and service quality are low and uneven. For connectivity, the initial benchmark will draw on administrative data and recognised international compendia; as a reference point, independent syntheses reported internet use around seven per cent in early 2023—an order of magnitude that justifies affordability measures and careful sequencing while local statistics systems mature ([DataReportal, “Digital 2023: South Sudan”](#)). Baselines in digital government and education will be derived from facility-level assessments and ministry records, with documentary evidence preserved as records under the information-governance chapter; in each case, MEL will cite the instrument and the date of collection to make the numbers contestable rather than rhetorical. The ESF and ISS require that risk screening, stakeholder engagement records, and grievance data be disclosed; MEL will therefore treat these as first-class datasets rather than annexes, and will publish them in an accessible register alongside results reports ([World Bank ESF](#); [AfDB ISS update](#)).

Indicators and verification logic. Indicators will be written in plain, testable terms (a numerator, a denominator, a time-bound target), with sources and methods stated in each results report. Wherever possible, they will be linked to observable administrative traces: service-uptime and usage logs for e-Government; device enrolment and learning-platform usage for universities and TVETs; lit-fibre nodes, active ISPs, and wholesale price/quality for broadband; publication completeness and timeliness for procurement; and screening and instrument delivery for safeguards. Verification will combine internal DQA routines with independent checks for high-stakes indicators, such as ISO/IEC 27001 certifications or large coverage claims, following the ESF/ISS expectation of proportionate, risk-based oversight ([World Bank ESF](#); [AfDB ISS press note and policy set]).

Data quality, integrity, and traceability. The MEL data model will require that each indicator observation be accompanied by a source reference, a collection date, a method statement, and a reviewer identity. Logically, this sits on top of the audit-trail requirements already specified for information governance; every change to a figure will leave a time-stamped footprint. To close the accountability loop between money and results, MEL will rely on the OCDS “ocid” and release IDs to link contracts, amendments, and implementation notes to the outputs they finance, allowing external parties to replicate data-joins and produce their own analyses ([OCDS canonical docs](#); [World Bank OCDS guidance note](#)). Where a result depends on stakeholder engagement or grievance resolution, MEL will cite the relevant ESF or ISS instrument and the public disclosure date to demonstrate compliance with safeguards’ transparency norms ([World Bank ESF](#); [AfDB ISS](#)).

Reporting and disclosure cadence. The facility will produce quarterly progress reports that narrate delivery against plan, cash execution, risks, and mitigation, and an annual results report that aggregates outcomes, disaggregations (sex, age, disability, rural/urban where applicable), and lessons learned. A public dashboard will present the same material in near real time, but without derogating from the primacy of the formally issued reports. All releases will be published on SUDESA’s portal in machine-readable formats, with lawful, narrowly tailored redactions for privacy, security, or commercial sensitivity as required by the data-protection framework and the procurement-transparency policy. This approach is consistent with the ESF’s emphasis on timely, meaningful disclosure and on grievance mechanisms that people can actually use, and with the AfDB’s strengthened requirements for stakeholder engagement and community health and safety in high-risk operations ([World Bank ESF overview](#); [AfDB ISS effectiveness announcement](#)).



Mid-term and final evaluation design. By Year Five, the Mission will commission an independent mid-term evaluation that interrogates relevance, effectiveness, efficiency, coherence, impact-likelihood, and sustainability prospects under the 2019 **OECD-DAC criteria**, including distributional questions that matter in low-income, rural contexts. The evaluation will be asked explicitly to consider whether the affordability measures and open-access regime have altered market structure in a way that is consistent with long-run consumer welfare and with the safeguards' commitments to inclusion; it will also be asked to test whether the education investments are yielding observable, attributable changes in learning behaviours and progression. By Year Ten, the final evaluation will assess realised impact and the durability of institutions, with counterfactual reasoning where feasible and at least a rigorous contribution analysis where it is not. The terms of reference will cite the DAC definitions and principles to avoid rote, box-ticking exercises and to ensure that findings and recommendations are usable by decision-makers rather than generic ([OECD DAC adapted definitions](#); operational guidance for applying the criteria thoughtfully ([resource index](#))).

Learning, adaptation, and remedy. MEL's purpose is not only to audit but to improve. The results and evaluation findings will flow into the Decision Register of the DTSC and the JSC, where management actions are recorded with deadlines, owners, and evidence of completion. Where a target is missed or a harm is identified, the system must show—in the public record—what corrective action was taken and on what date. This is consistent with the ESF's adaptive-risk management and with the AfDB's intent, in updating the ISS, to tighten alignment with other MDBs on community health and safety, gender-based violence, and stakeholder engagement expectations ([World Bank ESF note on adaptive risk management](#); [AfDB ISS effectiveness press release summarising the updates](#)).

Statistical strengthening and independence. Because several indicators rely on national statistics that are still being developed, MEL will invest—through the facility—in strengthening administrative data systems and survey capacity. Until those systems mature, it will triangulate with reputable international series so that directional claims are not built on wishful thinking; for connectivity, for instance, the DataReportal country pages and other neutral compendia provide transparent, cited numerators and denominators that can be cross-checked as national surveys begin publishing regular series ([DataReportal, South Sudan country page](#); an index of recent global updates for methodological transparency ([DataReportal hub](#))). MEL's independence is safeguarded by line-of-sight to the JSC and by the publication duty; where an indicator is politically sensitive, the answer is not suppression but methodologically sound presentation with an audit trail.

Conclusion. In sum, MEL is the State's warranty that claims made in the Mission Plan are tethered to facts that can be examined and, if necessary, contested. By aligning with the **OECD-DAC criteria** for evaluative judgement, by meeting the disclosure and engagement duties under the **World Bank ESF** and the **AfDB ISS**, and by linking finance, contracts, and results through **OCDS** identifiers, the regime ensures that learning is not a slogan but a documented, public practice.

13. Risk Management and Contingency Planning

13.1 Strategic, Operational, and Fiduciary Risks

Risk management under this Mission is governed by a single, enterprise-wide regime that follows the principles, framework, and process set out in **ISO 31000**. In practice, that means risks are identified in context, analysed for likelihood and consequence, evaluated against explicit criteria, treated through proportionate controls, and then monitored and communicated through formal reporting lines to the DTSC and JSC. The standard is not a checklist; it is a governance discipline that embeds risk thinking

into strategy, planning, budgeting, procurement, and disclosure, and it remains the reference for how risks are expressed, escalated, and reviewed across the programme life cycle.

Strategically, the programme faces risks of policy discontinuity, affordability shortfalls during the initial uptake period, and market structure frictions as open-access wholesale models mature. These translate operationally into delivery risks (civil-works delays, supply-chain interruptions, and skills bottlenecks) and fiduciary risks (cost escalation, ineligible expenditure, misprocurement, or integrity breaches). The **COSO Internal Control—Integrated Framework** supplies the internal-control vocabulary and components (control environment, risk assessment, control activities, information/communication, and monitoring) that implementing entities must evidence, while the Supreme Audit Institution's work is anchored in **INTOSAI's ISSAI 100** principles to ensure public-sector assurance over financial, compliance, and performance dimensions. Together, these frameworks define how risks are prevented, detected, disclosed, and corrected within an auditable system of control.

Environmental and social risks—community health and safety during trenching, labour influx, SEA/SH exposure, land access conflicts, and e-waste externalities—are classified and instrumented under the **World Bank Environmental and Social Framework (ESF)** and the **African Development Bank's updated Integrated Safeguards System (ISS)**. These regimes require risk-based screening, proportionate mitigation instruments, stakeholder engagement, and grievance mechanisms, and are explicitly designed to operate adaptively as circumstances change. Our programme treats those obligations as part of the core risk register rather than a parallel process.

13.2 Cyber, Data, and Continuity Risks

Cyber and data risks are governed through the **NIST Cybersecurity Framework 2.0** for outcome-oriented risk management and by a certifiable **ISO/IEC 27001:2022** information-security management system for control design, operation, and continual improvement. The CSF clarifies governance, identifies the relevant risk outcomes across Govern–Identify–Protect–Detect–Respond–Recover, and provides a common language for executives and engineers; ISO/IEC 27001 supplies the management-system engine that drives risk assessment, control selection, competence, internal audit, and corrective action. This twin track ensures that ministries can communicate risk credibly and that auditors can test the operating effectiveness of controls.

Continuity risks—power failures, network cuts, data-centre incidents, or force-majeure disruptions—are addressed through a documented and exercised **Business Continuity Management System** aligned with **ISO 22301:2019**. The BCMS establishes recovery objectives, impact analyses, continuity strategies, and exercise regimes, so that critical services can be restored within agreed windows and with evidence that plans are current, tested, and resourced. Cyber incident response remains methodologically aligned to the CSF's Respond/Recover functions and is operationalised in Government-CERT playbooks, but continuity and crisis-management responsibilities are deliberately broader than cyber and are rehearsed at ministerial and facility levels.

13.3 Mitigation Measures and Contingency Reserves

Mitigation follows the ISO 31000 hierarchy: avoid where feasible (for example, through route redesign to eliminate high-risk wayleaves), reduce through controls and standards (security baselines, segregation of duties, DPIAs, safeguards instruments), share where appropriate (insurance, warranties, and performance bonds), and accept within approved tolerances where residual risks are immaterial to objectives. The ESF's emphasis on risk-based and adaptive management is implemented literally: screening outcomes dictate instruments and monitoring intensity; stakeholder engagement and

grievance data are published, and new facts trigger mid-course corrections without waiting for fixed calendar reviews.

Fiduciary and integrity risks are mitigated at source through open competition and comprehensive disclosure. Every contracting process is published end-to-end in the **Open Contracting Data Standard (OCDS)** so that the public and partners can link planning, tender, award, contract, and implementation events over time. That transparency is not ornamental; the dataset is actively analysed for **procurement red flags**—submission patterns, sole-source anomalies, truncated timelines, repeated awards, or implementation deviations—using methods documented by the Open Contracting Partnership and corroborated by international guidance. Findings feed back into ex-ante controls and, where warranted, into investigations, sanctions, or design changes.

Financially, the facility maintains explicit **contingency reserves**. At the portfolio level, a controlled unallocated margin covers systemic shocks (FX, inflation spikes, or extraordinary logistics costs). At the contract level, variation ceilings are set ex-ante, governed per COSO's control-activities discipline, and any draw on contingency is disclosed in the OCDS implementation record with justification. Those reserves are calibrated annually in light of risk history and external conditions, and their use is reported to the JSC and external auditors under the SAI's mandate.

13.4 Risk Register Governance

The risk register is a living instrument, not a document of convenience. Ownership resides with the SUDESA Secretariat, but governance is distributed deliberately: strategic and fiduciary risks are reviewed by the JSC (with its Audit & Risk Subcommittee applying COSO's internal-control perspective and the SAI testing assurance under **ISSAI 100**), while cyber and continuity risks are reviewed by the DTSC against the CSF 2.0 outcomes, ISO/IEC 27001 non-conformities, and ISO 22301 exercise results. Each entry states the risk statement, cause, consequence, inherent rating, existing controls, treatment plan, owner, due date, and residual rating; each change leaves an audit trail.

Updates follow a defined cadence. Material events—serious incidents, audit findings, safeguards non-compliance, or procurement red-flag escalations—trigger immediate register changes and management actions; otherwise, monthly operating reviews and quarterly portfolio reviews suffice. The ESF and ISS impose their own disclosure and engagement duties; accordingly, safeguards-related risks and grievances appear in the same register and are disclosed to the public with lawful, narrowly tailored redactions, preserving both transparency and rights. This alignment ensures that risk is not split into financial, technical, and social silos but is held in one governance line of sight, with evidence that controls are designed, implemented, monitored, and—when they fail—strengthened.

Result. With ISO 31000 as the governing philosophy, COSO and ISSAI 100 as the assurance spine, CSF 2.0 and ISO/IEC 27001 for cyber risk, ISO 22301 for continuity, ESF/ISS for social and environmental safeguards, and OCDS plus red-flag analytics for integrity, the Mission's risk system is capable of anticipating shocks, absorbing surprises, and learning from failure in public view—precisely the posture required to steward a decade-long digital transformation responsibly.

[ISO 31000:2018 - Risk management — Guidelines](#)

[PowerPoint Timesaver Better charts, tables, and diagrams for better reports and presentations](#)

[ISSAI-100-Fundamental-Principles-of-Public-Sector-Auditing-1.pdf](#)

[Environmental and Social Framework \(ESF\)](#)

14. Stakeholder Engagement and Communications

This chapter defines the architecture for structured engagement and transparent communication with all constituencies whose decisions, resources, or trust determine the Mission's success. The approach is codified in the Stakeholder Engagement Plan (SEP) and Disclosure Policy, both of which are binding under the Host Country Agreement and the DTIF Charter. It aligns with World Bank ESF (ESS10) and AfDB ISS requirements for meaningful consultation, grievance redress, and public disclosure, while incorporating best practice in development finance and corporate governance.

14.1 Government, Parliament, and Sub-National Interfaces

The Mission's legitimacy depends on sustained political sponsorship and institutional coherence. Engagement with the Office of the President and the Council of Ministers ensures that digital transformation remains a national priority insulated from short-term political cycles. Parliamentary committees—particularly those on ICT, Finance, and Education—receive structured briefings and disclosure packs to enable informed oversight and appropriation decisions. At the sub-national level, governors and county commissioners are engaged through regional forums and technical working groups to coordinate civil works, rights-of-way, and school connectivity. These interfaces are not ceremonial; they are decision-rights forums where implementation bottlenecks are surfaced and resolved in real time, and where accountability for safeguards and grievance handling is demonstrated.

14.2 Development Partners and Private Sector

The financing architecture relies on a coalition of multilateral and bilateral partners—including the African Development Bank, World Bank, and Nordic Development Fund—and on Nordic DFIs such as Finnfund and Swedfund, whose mandates explicitly cover digital infrastructure and inclusive growth. Engagement with these partners is formalised through the DTIF governance structure: quarterly portfolio reviews, joint fiduciary and safeguards missions, and disclosure of financial and performance data in IPSAS-compliant statements and OCDS-formatted procurement releases. Private-sector actors—equipment vendors, systems integrators, ISPs, and local contractors—are engaged through open, competitive processes and through structured industry dialogues convened by SUDESA to refine technical standards, interoperability profiles, and service-quality benchmarks. This dual track—development finance for risk capital and private operators for execution—anchors the Mission's blended-finance model and its commitment to open access and vendor neutrality.

14.3 Civil Society, Traditional and Faith Leaders, and Diaspora

Digital transformation will fail if it is perceived as an elite project. Civil society organisations are therefore engaged from design through monitoring, with representation in thematic consultations on data protection, education inclusion, and community health and safety. Traditional authorities and faith leaders are briefed and mobilised as trusted intermediaries for community awareness on trenching safety, grievance channels, and the social value of connectivity. The diaspora—often a source of both remittances and technical expertise—is targeted through dedicated communication streams and volunteer programmes, creating a constituency that can amplify the Mission's legitimacy and contribute skills to local capacity building.

14.4 Public Communications, Branding, and Disclosure

The Mission's communications strategy rests on three pillars: transparency, accessibility, and trust. All non-confidential decisions, procurement data, safeguards instruments, and performance reports are published on the SUDESA portal in machine-readable formats, with lawful, narrowly tailored redactions for privacy, security, or commercial sensitivity. A public dashboard visualises key indicators—coverage,

affordability, service uptime, grievance resolution—so that citizens and partners can track progress without waiting for formal reports. Branding guidelines ensure that all materials convey the Mission’s identity as a national, inclusive, and future-oriented undertaking, while avoiding donor fragmentation or vendor capture. Disclosure obligations mirror those in the World Bank ESF and AfDB ISS, and are reinforced by the DTIF Charter’s transparency clauses and the open-contracting policy. Grievance redress mechanisms are advertised through multiple channels—web, SMS, radio, and community meetings—so that affected people can seek remedy without procedural or technological barriers.

Result: Stakeholder engagement under this framework is not episodic but institutionalised. It creates predictable forums for decision-makers, credible disclosure for financiers, voice and remedy for citizens, and a coherent narrative for the public. By aligning with global safeguards and open-government norms, the Mission converts transparency from a compliance burden into a strategic asset that sustains trust over a decade of transformation.

15. Alignment with Various Agendas

15.1 Alignment with the United Nations Sustainable Development Goals (SDGs)

The SUDESA Mission Plan is fully aligned with the 2030 Agenda for Sustainable Development, ensuring that its objectives and implementation strategies contribute to the achievement of key Sustainable Development Goals. The digitalisation of government systems and the deployment of broadband infrastructure directly advance SDG 9 on industry, innovation, and infrastructure, while the Education Digitalisation Programme operationalises SDG 4 on quality education by embedding digital literacy and equitable access to learning resources across all levels of the education system. Governance reforms, fiduciary transparency measures, and cybersecurity frameworks embedded in the Digital Government Blueprint are consistent with SDG 16, which calls for peace, justice, and strong institutions. Furthermore, the financing architecture, particularly the Digital Transformation Investment Facility (DTIF), reflects the spirit of SDG 17 by fostering multi-stakeholder partnerships and mobilising blended finance for sustainable development. These alignments ensure that South Sudan’s digital transformation contributes to the global commitment to eradicate poverty, reduce inequality, and promote inclusive growth (United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, 2015).

15.2 Alignment with the African Union Agenda 2063

The Mission Plan is equally consonant with the African Union’s Agenda 2063, which articulates the vision of “The Africa We Want.” The strategic objectives of SUDESA resonate with Aspiration 1, which seeks inclusive growth and sustainable development, through the establishment of sovereign digital infrastructure and the modernisation of agriculture under the SSSFPS-EI framework. The governance and compliance architecture, including the adoption of open contracting standards and the enactment of data protection and cybersecurity legislation, advances Aspiration 3 on good governance, democracy, and respect for human rights. Moreover, the emphasis on digital literacy, youth empowerment, and gender inclusion reflects Aspiration 6, which prioritises people-driven development and the unleashing of Africa’s human capital (African Union Commission, *Agenda 2063: The Africa We Want*, 2015).

15.3 Alignment with the Social Global Goals (SGGs) under Agenda for Social Equity 2074

Beyond these global and continental frameworks, the Mission Plan is anchored in the Agenda for Social Equity 2074, which serves as the long-term normative and compliance framework for all programs executed under the Strategic Engagement Agreement between the Government of South Sudan and



the European Social Label (EUSL). Agenda 2074 consolidates and extends the ambitions of the SDGs and Agenda 2063 into a unified horizon, structured around seventeen Social Global Goals (SGGs) that prioritise universal access to essential services, educational equity, social justice, and ethical technology governance. The operationalisation of these principles within SUDESA is evident in the integration of zero-trust security models, fiduciary transparency mechanisms, and inclusive education strategies. By embedding Agenda 2074 into the governance and financing architecture of the Mission Plan, South Sudan ensures policy continuity beyond electoral cycles, thereby mitigating the risks of political volatility and safeguarding the integrity of long-term investments (Creativa Center, *Agenda for Social Equity 2074 Framework*, 2025).

15.4 Financing and Compliance Anchoring under Agenda 2074

The financing and compliance architecture of the Mission Plan is explicitly anchored in Agenda 2074. All disbursements under the DTIF are conditioned upon adherence to fiduciary standards, environmental and social safeguards, and monitoring and evaluation protocols consistent with the African Development Bank's Integrated Safeguards System (ISS) and the World Bank Environmental and Social Framework (ESF). This alignment not only secures eligibility for concessional finance and grant-based instruments but also positions South Sudan as a credible partner for Nordic development finance institutions and other strategic actors. By institutionalising Agenda 2074 as the non-negotiable baseline for compliance and reporting, the Mission Plan transforms digitalisation from a technical exercise into a sovereign strategy for equity, resilience, and sustainable growth.

1. Global and Continental Agendas

- United Nations Sustainable Development Goals (SDGs):
<https://sdgs.un.org/2030agenda>
- African Union Agenda 2063:
<https://au.int/en/agenda2063>
- Agenda for Social Equity 2074 (internal reference):
[Creativa Center Framework – internal document]
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention):
<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

2. Digital Transformation and Procurement Standards

- UNCITRAL Model Law on Public Procurement (2011):
https://uncitral.un.org/en/texts/procurement/modellaw/public_procurement
- World Bank Procurement Regulations for IPF Borrowers (Nov 2020):
<https://thedocs.worldbank.org/en/doc/178331533065871195-0290022020/original/ProcurementRegulations.pdf>
- Open Contracting Data Standard (OCDS):
<https://standard.open-contracting.org/latest/en/>



3. Fiduciary and Financial Management

- International Public Sector Accounting Standards (IPSAS):
<https://www.ipsasb.org/publications/2024-handbook-international-public-sector-accounting-pronouncements>
- INTOSAI ISSAI 100 – Fundamental Principles of Public-Sector Auditing:
<https://www.issai.org/wp-content/uploads/2019/08/ISSAI-100-Fundamental-Principles-of-Public-Sector-Auditing-1.pdf>
- International Standards on Auditing (ISA 700 Revised):
<https://www.iaasb.org/publications/international-standard-auditing-isa-700-revised-forming-opinion-and-reporting-financial-statements>

4. ESG and Safeguards

- World Bank Environmental and Social Framework (ESF):
<https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>
- African Development Bank Integrated Safeguards System (ISS) – Updated 2024:
<https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>
- IFC Performance Standards on Environmental and Social Sustainability:
https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/policies-standards/performance-standards

5. Cybersecurity and Data Governance

- NIST Cybersecurity Framework 2.0:
<https://www.nist.gov/cyberframework>
- ISO/IEC 27001:2022 Information Security Management:
<https://www.iso.org/standard/27001>

6. Monitoring, Evaluation, and Learning (MEL)

- OECD DAC Evaluation Criteria (2019):
[https://one.oecd.org/document/DCD/DAC\(2019\)58/FINAL/en/pdf](https://one.oecd.org/document/DCD/DAC(2019)58/FINAL/en/pdf)
- World Bank – Ten Steps to a Results-Based M&E System:
<https://documents1.worldbank.org/curated/en/638011468766181874/pdf/296720PAPER0100steps.pdf>
- DCED Standard for Results Measurement:
<https://www.enterprise-development.org/dced-guidance/dced-standard-results-measurement/>

7. Dispute Resolution and Arbitration

- UNCITRAL Mediation Rules (2021):
https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/22-01369_mediation_rules_ebook_1.pdf



- UNCITRAL Arbitration Rules (2013):
<https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/uncitral-arbitration-rules-2013-e.pdf>
- ICC Rules of Arbitration (2021):
<https://iccwbo.org/dispute-resolution/dispute-resolution-services/arbitration/rules-procedure/2021-arbitration-rules/>
- New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958):
<https://www.newyorkconvention.org/contracting-states>

16. SWOT Analysis (Digital, Education, and Broadband)

16.1 Strengths and Weaknesses

South Sudan's digital transformation agenda, as articulated through SUDESA, benefits from several inherent strengths. Foremost among these is the presence of strong political will and high-level endorsement, evidenced by the Government's formal commitment to the Social Digital Equity Program (SDEP) and the establishment of SUDESA as a semi-autonomous institutional mechanism. This political alignment provides a stable foundation for long-term planning and resource mobilisation. Another critical strength lies in the country's greenfield status: the absence of entrenched legacy systems allows for the adoption of modern, cloud-native, and mobile-first solutions without the burden of costly retrofitting. Furthermore, there is growing interest from Nordic and multilateral development partners in supporting digital governance and inclusion in fragile states, creating a favourable environment for blended finance and technical cooperation.

However, these strengths are counterbalanced by significant weaknesses. The most pressing challenge is the severe infrastructure deficit, particularly in rural areas where broadband penetration remains extremely low. This gap not only constrains connectivity but also limits the scalability of digital services. Additionally, digital literacy levels across the population are markedly low, with limited integration of ICT in education and public administration. Institutional capacity to manage complex ICT systems is also underdeveloped, raising concerns about sustainability and operational resilience. These weaknesses underscore the need for phased implementation, targeted capacity building, and strong technical partnerships to mitigate systemic risks.

16.2 Opportunities and Threats

The opportunities presented by this transformation are substantial. South Sudan has one of the youngest populations in the world, offering a demographic dividend if digital skills and entrepreneurship can be scaled effectively. The integration of digital tools into education systems, combined with vocational training and device distribution, positions the country to build a digitally literate workforce capable of driving innovation and economic diversification. Regionally, South Sudan's membership in COMESA and alignment with the African Union's Agenda 2063 create pathways for cross-border digital trade, interoperability, and policy harmonisation. At the global level, the increasing prioritisation of digital public infrastructure by development partners provides access to concessional finance, technical assistance, and knowledge-sharing platforms.

Conversely, the initiative faces external threats that must be proactively managed. Political instability remains a persistent risk, with the potential to disrupt implementation timelines and erode investor confidence. Cybersecurity vulnerabilities pose another critical threat, particularly in the absence of robust legal frameworks for data protection and digital rights. Additionally, there is a risk of digital

exclusion if access to broadband and devices is not equitably distributed, potentially exacerbating existing social inequalities. These threats necessitate a comprehensive risk management strategy, including the enactment of enabling legislation, the adoption of Zero Trust security models, and the institutionalisation of inclusive access policies.

SWOT Table

Factor	Description
Strengths	Strong political will and high-level endorsement; greenfield opportunity enabling modern, scalable design; growing interest from Nordic and multilateral partners.
Weaknesses	Severe infrastructure gaps, especially in rural areas; low digital literacy; limited institutional capacity to manage ICT systems.
Opportunities	Large youthful population for digital skills development; regional integration through COMESA and Smart Africa; global momentum for digital public infrastructure and blended finance.
Threats	Political instability and implementation disruption; cybersecurity vulnerabilities; risk of digital exclusion if access is inequitable.

17. PESTEL Analysis

17.1 Political and Economic

Political:

South Sudan's political environment is characterised by both opportunity and fragility. On one hand, the Government has demonstrated strong commitment to digitalisation, as evidenced by the formal endorsement of the Social Digital Equity Program (SDEP) and the establishment of SUDESA as a semi-autonomous institutional mechanism. This political will is a critical enabler for long-term transformation, ensuring alignment with national development strategies and peacebuilding frameworks such as the Revitalized Agreement on the Resolution of the Conflict in South Sudan (R-ARCSS). However, the risk of political instability remains significant. Leadership transitions, inter-communal tensions, and governance challenges could disrupt implementation timelines and erode investor confidence. Sustained political stability, cross-party consensus, and institutional anchoring through legislation will therefore be essential to safeguard continuity and credibility.

Economic:

The economic context presents a dual reality. South Sudan faces severe fiscal constraints, with limited domestic revenue and high dependency on oil exports, which exposes the economy to volatility in global commodity markets. Inflationary pressures and currency instability further complicate the macroeconomic environment. Despite these challenges, digitalisation offers a pathway to economic diversification, job creation, and improved public sector efficiency. The development of a local ICT ecosystem, combined with vocational training and entrepreneurship programs, can stimulate inclusive growth and reduce reliance on extractive industries. Moreover, strong donor engagement and the availability of concessional finance from institutions such as the African Development Bank (AfDB), the

World Bank, and Nordic development partners create a favourable environment for blended finance models that can underwrite the costs of digital infrastructure and capacity building.

17.2 Social and Technological

Social:

South Sudan's demographic profile is both a challenge and an opportunity. With one of the youngest populations globally, the country faces urgent demands for education, employment, and social inclusion. Digital transformation, if implemented inclusively, can serve as a catalyst for addressing these needs by expanding access to education, enabling remote learning, and fostering youth entrepreneurship. However, low digital literacy, gender disparities, and the marginalisation of vulnerable groups—including internally displaced persons (IDPs) and persons with disabilities—pose significant risks of digital exclusion. The success of the transformation will depend on targeted interventions such as national digital literacy campaigns, gender-responsive programming, and community-based outreach to ensure equitable access and participation.

Technological:

The technological landscape offers a unique leapfrogging opportunity. South Sudan's greenfield status—marked by the absence of entrenched legacy systems—allows for the adoption of cloud-native, mobile-first, and open standards-based solutions. Strategic partnerships with global technology providers such as Microsoft, combined with the deployment of satellite broadband solutions like Starlink, can accelerate connectivity and service delivery even in remote areas. However, the lack of domestic technical capacity, coupled with limited local manufacturing and assembly capabilities, underscores the need for robust capacity-building programs and structured technology transfer mechanisms. Cybersecurity vulnerabilities also represent a critical concern, necessitating the early adoption of Zero Trust architectures, ISO 27001 standards, and a comprehensive national cybersecurity strategy.

17.3 Environmental and Legal

Environmental:

The environmental dimension of digital transformation in South Sudan is twofold. On the one hand, the deployment of digital infrastructure—such as data centres and broadband networks—carries environmental risks, including energy consumption and e-waste generation. On the other hand, digitalisation can contribute to environmental sustainability by enabling climate-smart agriculture, improving disaster preparedness, and reducing the carbon footprint of public administration through paperless systems. The integration of green technologies, energy-efficient devices, and e-waste management protocols into the implementation strategy is therefore essential. These measures align with both the European Green Deal and the sustainability objectives of Agenda for Social Equity 2074.

Legal:

The legal environment is currently underdeveloped, with no comprehensive frameworks governing data protection, digital identity, cybersecurity, or digital procurement. This regulatory vacuum poses significant risks to privacy, security, and fiduciary integrity. At the same time, it presents an opportunity to design modern, rights-based legal instruments from the ground up, aligned with international best practices and regional instruments such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The enactment of a Data Protection and Privacy Act, a Digital Identity Law, and a Public Procurement Reform Act will be critical to ensuring compliance, building public trust, and attracting investment. These laws must be developed through inclusive

consultation processes and supported by institutional capacity-building to ensure effective enforcement.

PESTEL Analysis Table – South Sudan (Digitalisation, Education, and Broadband)

Factor	Key Considerations
Political	Strong government commitment to digitalisation and SUDESA establishment; alignment with peace agreements; risk of political instability and governance fragmentation.
Economic	Limited fiscal space and heavy reliance on oil revenues; inflation and currency volatility; opportunities for economic diversification through digital economy and blended finance.
Social	Young population offering demographic dividend; urgent need for education and employment; risks of digital exclusion due to low literacy, gender disparities, and marginalisation of vulnerable groups.
Technological	Greenfield opportunity for cloud-native and mobile-first solutions; potential for leapfrogging via satellite broadband and partnerships with global tech firms; cybersecurity vulnerabilities and limited local technical capacity.
Environmental	Risks from energy consumption and e-waste linked to digital infrastructure; opportunities for climate-smart agriculture and reduced carbon footprint through digital governance; need for green technologies and e-waste management protocols.
Legal	Absence of comprehensive digital laws (data protection, cybersecurity, digital ID, procurement); opportunity to design modern, rights-based frameworks aligned with international standards and AU Malabo Convention.

18. Legal and Policy Roadmap

The digital transformation of South Sudan requires a coherent legal and regulatory framework that guarantees compliance, protects fundamental rights, and ensures institutional accountability. This roadmap consolidates the legislative priorities identified in the Strategic Engagement Agreement, the Host Country Agreement, and the governance instruments of SUDESA and GSIA. It is fully aligned with Agenda for Social Equity 2074, the African Union's Agenda 2063, and international standards such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), ISO/IEC 27001, and the Open Contracting Data Standard (OCDS).

18.1 Data Protection & Privacy Act

The first legislative priority is the enactment of a Data Protection and Privacy Act. This statute will establish the principles of lawful, fair, and transparent processing of personal data, define the rights of data subjects, and impose obligations on data controllers and processors. It will create a National Data Protection Authority vested with enforcement powers, including the authority to impose administrative sanctions and conduct compliance audits. The Act will align with the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) (<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>)

and incorporate elements of the General Data Protection Regulation (GDPR) adapted to the South Sudanese context. It will also mandate data sovereignty, requiring that sensitive government and citizen data be hosted within national or trusted regional jurisdictions, supported by sovereign data centres and hybrid cloud solutions.

18.2 Digital Identity Act

The second legislative instrument is the Digital Identity Act, which will provide the legal foundation for a unified, secure, and interoperable national digital identity system. This law will confer legal recognition on digital identity as equivalent to physical identity for all public services and transactions. It will establish governance structures for identity issuance, authentication, and lifecycle management, incorporating privacy-by-design and security-by-design principles to protect biometric and personal data. The Act will enable integration with civil registration systems and ensure interoperability with regional frameworks under the African Union Digital ID Strategy (<https://au.int/en/documents/20200904/digital-transformation-strategy-africa-2020-2030>).

18.3 Cybersecurity Law and CERT Designation

Cybersecurity is a matter of national security and public trust. The Cybersecurity Act will define national cybersecurity standards for critical infrastructure, government systems, and private sector operators of essential services. It will mandate the adoption of Zero Trust Architecture, ISO/IEC 27001 (<https://www.iso.org/standard/27001>), and the NIST Cybersecurity Framework (<https://www.nist.gov/cyberframework>) across all government platforms. The Act will establish a National Cybersecurity Authority and formally designate a Computer Emergency Response Team (CERT) responsible for threat intelligence, incident response, and cross-border coordination. It will also introduce criminal and civil liabilities for cybercrime, including hacking, identity theft, and data breaches, supported by judicial capacity-building.

18.4 E-Procurement and Open Contracting Reforms

To enhance transparency, efficiency, and accountability in public procurement, the roadmap mandates the adoption of a **Public Procurement Reform Act**. This law will require the use of digital procurement platforms integrated with compliance tools for real-time monitoring and anomaly detection. It will mandate the publication of procurement data in accordance with the **Open Contracting Data Standard (OCDS)** (<https://standard.open-contracting.org/latest/en/>), covering all stages from planning to implementation. The Act will align with the **UNCITRAL Model Law on Public Procurement** (https://uncitral.un.org/en/texts/procurement/modellaw/public_procurement) and the procurement frameworks of multilateral development banks, ensuring compliance with international fiduciary standards.

18.5 Broadband and Spectrum Policy; Building Regulations

Connectivity is recognised as a social right and an economic enabler. The **National Broadband Strategy** will define spectrum allocation policies, universal service obligations, and affordability benchmarks to ensure inclusive access. It will introduce licensing frameworks for local broadband resellers and Internet Service Providers to promote competition and last-mile connectivity. The strategy will also mandate the integration of digital readiness into building codes and infrastructure regulations, including the installation of fibre ducts in new roads and compliance with smart grid standards. These measures will align with the **African Union Digital Transformation Strategy (2020–2030)** (<https://au.int/en/documents/20200904/digital-transformation-strategy-africa-2020-2030>) and COMESA's Digital Free Trade Area standards to facilitate regional interoperability.

Institutional Anchoring and Compliance

The implementation of these legal instruments will be anchored in the governance structures of SUDESA, particularly the Digital Transformation Steering Committee and the Joint Steering Committee, with fiduciary oversight provided by the Digital Transformation Investment Facility. Compliance will be monitored through quarterly reporting, independent audits, and adherence to the environmental and social safeguards of the African Development Bank (<https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>) and the World Bank Environmental and Social Framework (<https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>). All legislative drafting processes will be inclusive, transparent, and supported by capacity-building programs for legal and regulatory institutions, ensuring that the digital transformation of South Sudan is not only technologically sound but also legally robust and socially equitable.

19. Capacity Building and Change Management

The sustainability of South Sudan's digital transformation depends not only on infrastructure and legal frameworks but also on the development of human capital, institutional reform, and cultural adaptation within the public sector and the broader ecosystem. This chapter outlines the strategic measures required to build competencies, reform organisational structures, and foster a culture of innovation and accountability, ensuring that the transformation is inclusive, resilient, and future-proof.

19.1 Civil Service Digital Competencies

The first priority is the systematic development of digital competencies across the civil service. This involves equipping public officials with the knowledge and skills necessary to operate within a secure, interoperable, and data-driven environment. Training programs will cover foundational digital literacy, cybersecurity awareness, and the use of enterprise-grade platforms such as Microsoft 365 Government Suite and Azure Government Cloud. Advanced modules will address data governance, e-procurement systems, and compliance monitoring. These programs will be delivered through a blended learning model combining in-person workshops, online courses, and certification pathways, aligned with international standards such as the European e-Competence Framework and the African Union Digital Transformation Strategy (<https://au.int/en/documents/20200904/digital-transformation-strategy-africa-2020-2030>).

19.2 Institutional Reform and Job Profiles

Digital transformation requires a fundamental reconfiguration of institutional structures and job profiles within the public sector. Ministries and agencies will establish dedicated ICT units responsible for system administration, cybersecurity, and data analytics. Job descriptions will be revised to incorporate digital competencies as core requirements, and performance evaluation frameworks will be updated to reflect the adoption of digital tools and compliance with governance standards. These reforms will be codified in a Digital Transformation Act, ensuring that institutional mandates, reporting lines, and accountability mechanisms are clearly defined. This approach aligns with global best practices in public sector modernisation and supports the objectives of Agenda for Social Equity 2074, particularly its emphasis on governance integrity and institutional resilience.

19.3 Local Vendor Ecosystem and Certification

The roadmap also prioritises the development of a robust local vendor ecosystem to reduce dependency on external suppliers and stimulate domestic economic growth. This will involve the accreditation of local ICT firms through a structured certification program that ensures compliance with

technical, fiduciary, and cybersecurity standards. Certified vendors will be eligible to participate in government procurement processes under the **Open Contracting Data Standard (OCDS)** framework (<https://standard.open-contracting.org/latest/en/>). Capacity-building initiatives will include training in cloud services, device management, and software development, supported by partnerships with global technology providers such as Microsoft. This strategy not only enhances supply chain resilience but also creates employment opportunities and fosters innovation within the national economy.

19.4 Leadership, Incentives, and Change Champions

Finally, the success of digital transformation hinges on leadership commitment and cultural change within the public sector. Senior officials will undergo executive training programs focused on digital governance, strategic ICT planning, and ethical technology use. Change management strategies will include the identification and empowerment of “digital champions” within ministries and agencies to drive adoption and peer learning. Incentive structures will be introduced to reward innovation, compliance, and performance in digital service delivery. These measures will be complemented by communication campaigns designed to build public trust and promote citizen engagement, ensuring that digital transformation is perceived not as a technical exercise but as a national mission for social equity and economic resilience.

20. Sustainability and Exit Strategy

The long-term success of South Sudan’s digital transformation depends on its ability to transition from externally supported implementation to nationally owned, locally governed, and financially sustainable systems. This chapter sets out the strategic measures required to ensure that the digital infrastructure, services, and institutions established through SUDESA endure beyond the initial program lifecycle and continue to evolve in response to national needs and global technological trends.

20.1 Operations and Maintenance (O&M) and Lifecycle Financing

The sustainability of digital systems requires a robust operations and maintenance framework supported by predictable financing mechanisms. All infrastructure components, including broadband networks, data centres, and e-Government platforms, will be governed by service-level agreements that define performance standards, maintenance schedules, and escalation protocols. Lifecycle costing will be integrated into the Digital Transformation Investment Facility (DTIF) to ensure that capital investments are complemented by adequate provisions for recurrent expenditures. Financing strategies will prioritise cost recovery through affordable service fees, public-private partnerships, and phased integration of domestic budget allocations. These measures will align with international fiduciary standards such as **IPSAS** (<https://www.ipsasb.org/publications/2024-handbook-international-public-sector-accounting-pronouncements>) and the governance principles of the African Development Bank Integrated Safeguards System (<https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>).

20.2 Institutionalisation within National Systems

Institutional sustainability will be achieved through the progressive integration of SUDESA’s functions into the permanent structures of government. This process will be guided by a Digital Transformation Act that codifies governance arrangements, reporting lines, and accountability mechanisms. Core functions such as cybersecurity, data governance, and procurement oversight will be embedded within relevant ministries and agencies, supported by statutory mandates and budgetary allocations. The transition plan will include capacity-building programs for civil servants, ensuring that institutional

knowledge is retained and operational continuity is maintained. This approach reflects the principles of **Agenda for Social Equity 2074**, which emphasises governance integrity and policy continuity beyond electoral cycles.

20.3 Handover, Local Ownership, and Cost Recovery

The exit strategy prioritises local ownership as a prerequisite for sustainability. This will involve the gradual transfer of operational responsibilities from international partners to national institutions, supported by structured knowledge transfer programs and technical assistance. Cost recovery mechanisms will be introduced to reduce dependency on external funding, including user fees for premium digital services, licensing revenues from broadband operators, and monetisation of non-sensitive government data under open data frameworks.

These measures will be implemented in compliance with the Open Contracting Data Standard (<https://standard.open-contracting.org/latest/en/>) and the fiduciary requirements of development finance institutions, ensuring transparency and accountability in revenue generation and expenditure.

20.4 Long-Term Governance and Strategic Adaptation

Sustainability also requires a governance model capable of adapting to technological, economic, and social changes. A National Digital Governance Authority will be established to oversee policy development, standards enforcement, and inter-agency coordination. This body will maintain strategic partnerships with regional and global institutions, including the African Union Digital Transformation Strategy (<https://au.int/en/documents/20200904/digital-transformation-strategy-africa-2020-2030>), to ensure alignment with emerging norms and best practices. Periodic strategic reviews will be conducted to assess performance, identify risks, and recalibrate priorities, supported by independent evaluations and stakeholder consultations. These mechanisms will guarantee that South Sudan's digital transformation remains resilient, inclusive, and future-ready.

Annex A: Acronyms and Glossary

This annex provides a consolidated list of acronyms and key terms used throughout the SUDESA Mission Plan to ensure clarity and consistency in interpretation.

Acronyms

AfDB – African Development Bank
AU – African Union
CERT – Computer Emergency Response Team
COMESA – Common Market for Eastern and Southern Africa
DTIF – Digital Transformation Investment Facility
DTSC – Digital Transformation Steering Committee
EUSL – European Social Label
ESF – Environmental and Social Framework (World Bank)
GDPR – General Data Protection Regulation
GSIA – Global Social Impact Alliance
ICT – Information and Communication Technology
IPSAS – International Public Sector Accounting Standards
ISO/IEC 27001 – International Standard for Information Security Management
JSC – Joint Steering Committee
MEL – Monitoring, Evaluation, and Learning
NIST CSF – National Institute of Standards and Technology Cybersecurity Framework
OCDS – Open Contracting Data Standard
PPP – Public-Private Partnership
R-ARCSS – Revitalized Agreement on the Resolution of the Conflict in South Sudan
SDGs – Sustainable Development Goals
SGGs – Social Global Goals (Agenda for Social Equity 2074)
SUDESA – South Sudan Development and Social Equity Agency
UNCTRAL – United Nations Commission on International Trade Law

Glossary of Key Terms

Agenda for Social Equity 2074 (Agenda 2074): A long-term strategic framework developed to unify global and continental agendas, including the SDGs and Agenda 2063, into a single horizon extending to 2074. It is anchored in seventeen Social Global Goals covering education, health, digital inclusion, governance, gender equality, and ethical technology use.

Digital Transformation Investment Facility (DTIF): A pooled financing mechanism established under SUDESA to mobilise, manage, and allocate resources for digital transformation initiatives, operating under IPSAS-compliant fiduciary standards and aligned with AfDB and World Bank safeguards.

Digital Identity: A legally recognised electronic identity enabling individuals to authenticate themselves and access public and private services securely, governed by the Digital Identity Act.

Open Contracting Data Standard (OCDS): An international standard for publishing structured data and documents at all stages of the contracting process to promote transparency, accountability, and public oversight.

Zero Trust Architecture: A cybersecurity model that assumes no implicit trust within a network and enforces strict identity verification and least-privilege access for all users and devices.

Data Sovereignty: The principle that data is subject to the laws and governance structures of the nation in which it is collected and stored, requiring local hosting of sensitive government and citizen data.

Annex E: Technical Annex – Enterprise Architecture and Standards

E.1 Purpose and Scope

This annex defines the enterprise architecture and technical standards that will govern the digital transformation of South Sudan's public sector under the SUDESA framework. It establishes the principles, reference models, and compliance requirements for all digital systems, ensuring interoperability, security, and scalability. The architecture is aligned with **Agenda for Social Equity 2074**, the **African Union Digital Transformation Strategy (2020–2030)**

<https://au.int/en/documents/20200904/digital-transformation-strategy-africa-2020-2030> and global best practices such as **TOGAF**, **ISO/IEC 27001**, and the **NIST Cybersecurity Framework** <https://www.nist.gov/cyberframework>

E.2 Architectural Principles

The enterprise architecture is guided by five foundational principles:

1. **Digital Sovereignty:** All core government systems and sensitive data must be hosted within national or trusted regional jurisdictions, supported by sovereign data centres and hybrid cloud models.
2. **Interoperability and Open Standards:** All platforms must adhere to open API standards and data exchange protocols to ensure seamless integration across ministries and agencies.
3. **Security by Design:** Cybersecurity measures, including Zero Trust Architecture, encryption, and multi-factor authentication, must be embedded from inception.
4. **Scalability and Modularity:** Systems must be designed for phased implementation and future expansion without requiring fundamental redesign.
5. **User-Centricity and Accessibility:** All digital services must be inclusive, multilingual, and compliant with accessibility standards for persons with disabilities.

E.3 Enterprise Architecture Layers

The architecture is structured across four interdependent layers:

Business Layer: Defines the functional domains of government operations, including civil registration, taxation, procurement, education, and health services. Business processes will be re-engineered to eliminate redundancies and enable digital workflows.

Application Layer: Comprises interoperable platforms for e-Government services, digital identity, and sector-specific applications. Core systems include:

- **Microsoft 365 Government Suite** for secure communication and collaboration.
- **Azure Government Cloud** for hosting national registries and critical applications.
- **Power Platform and Dynamics 365** for workflow automation and citizen engagement.

Data Layer: Establishes a unified data governance framework, including metadata standards, classification protocols, and retention policies. Data sovereignty will be enforced through local hosting and hybrid cloud configurations, with compliance to the **Malabo Convention** (<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>).

Technology Layer: Provides the physical and virtual infrastructure, including:



- National fiber optic backbone and satellite broadband for universal connectivity.
- Tier III or higher data centres with disaster recovery and failover capabilities.
- Secure endpoints (Surface devices) pre-configured with compliance and security tools.

E.4 Compliance and Security Standards

All systems must comply with the following standards:

- **ISO/IEC 27001** for information security management (<https://www.iso.org/standard/27001>).
- **NIST Cybersecurity Framework** for risk management and resilience.
- **Open Contracting Data Standard (OCDS)** for procurement transparency (<https://standard.open-contracting.org/latest/en/>).
- **UNCITRAL Model Law on Public Procurement** for legal harmonisation (https://uncitral.un.org/en/texts/procurement/modellaw/public_procurement).

Zero Trust principles will be mandatory across all layers, supported by Microsoft Compliance Center for real-time monitoring and audit trails.

E.5 Interoperability and Integration Framework

A **National Digital Architecture Council** will be established to oversee system integration, enforce interoperability standards, and approve all new digital initiatives. Integration will be achieved through:

- **Open APIs** for secure data exchange.
- **Enterprise Service Bus (ESB)** for orchestration of inter-agency workflows.
- **Data Interchange Standards** aligned with AU and COMESA frameworks.

E.6 Accessibility and Inclusion

All platforms must comply with **Web Content Accessibility Guidelines (WCAG 2.1)** and provide multilingual interfaces in English, Arabic, and major local languages. Special provisions will be made for assistive technologies to ensure inclusion of persons with disabilities.

E.7 Governance and Oversight

The Digital Transformation Steering Committee (DTSC) will serve as the primary governance body for enterprise architecture compliance. Quarterly audits will be conducted to verify adherence to standards, supported by independent assessments from accredited certification bodies.

Annex F (Legal Draft): Open Access Broadband — Technical and Regulatory Notes

Preamble.

This Annex forms an integral part of the SUDESA Instruments and binds all Public Bodies, Licensees and Participants operating electronic communications networks and services within the Republic of South Sudan where (a) public rights-of-way are used, (b) public funds or fiscal incentives are deployed, or (c) SUDESA-coordinated programmes apply. It shall be interpreted in harmony with the National Communications Act, 2012, the mandate of the National Communication Authority (NCA), and the SUDESA governance framework. [\[cite\]National Communications Act, 2012 \(official consolidated text\)\[NCA official website\]](#) SUDESA Strategic/Institutional framework (EUSL)[\[](#)

Article 1 — Purpose, Scope and Guiding Norms

1.1 Purpose. This Annex establishes a national open-access broadband regime to ensure non-discriminatory wholesale access to essential network facilities and services, accelerate universal, affordable, good-quality connectivity, and enable regional digital integration. It operationalises continental and international best practice, including the African Union Digital Transformation Strategy (2020–2030), ITU/Digital Regulation guidance on open access and infrastructure sharing, and recognised wholesale access models. [\[cite\]AU Digital Transformation Strategy 2020–2030\[ITU GSR Open Access Best-Practice\]\[ITU–World Bank Digital Regulation Handbook/Platform\]](#)

1.2 Scope. This Annex applies to: a) passive infrastructure and civil works; b) active wholesale services (e.g., dark fibre, wavelength, bitstream, VULA); c) mobile infrastructure sharing and small-cell neutral-host layers; d) spectrum usage and non-terrestrial networks (NTN) integration; and e) PPPs, publicly funded projects and any deployments benefitting from public rights or incentives. [\[cite\]\[ITU GSR Open Access Best-Practice\]](#)

1.3 Guiding Norms. Implementation shall uphold: (i) digital sovereignty and data localisation where required; (ii) interoperability and open standards; (iii) security-by-design and Zero Trust; (iv) scalability/modularity; and (v) user-centric accessibility. [\[cite\]\[AU Digital Strategy 2020–2030\]\[BEREC Open-Internet Guidelines \(transparency & QoS frameworks\)\]](#)

Article 2 — Definitions

2.1 Open Access means non-discriminatory, transparent access by third parties to network facilities/services to remove bottlenecks and promote effective competition. [\[cite\]\[ITU GSR Open Access Best-Practice\]](#)

2.2 Passive Infrastructure comprises ducts, poles, towers, masts, handholes/manholes, shelters, power, and dark fibre. **Active Infrastructure** comprises lit fibre, transmission electronics, and RAN equipment. [\[cite\]\[GSMA Infrastructure Sharing Overview\]](#)

2.3 Wholesale-Only (Neutral Host) Operator means an entity offering wholesale services exclusively, with no retail operations. [\[cite\]\[World Bank PPP Knowledge base – Network/Service Separation\]](#)

2.4 Bitstream and **VULA** mean, respectively, wholesale logical access and a virtual unbundled access with local handover enabling service differentiation. [\[cite\]\[EU Broadband Guidelines – wholesale products \(model reference\)\]](#)



2.5 **NTN** means non-terrestrial networks as integrated in the 3GPP 5G System. [\[cite\]3GPP/ETSI 5G Overview](#)

Article 3 — Institutional Roles and Hierarchy

3.1 **NCA.** The NCA remains the competent regulator for licensing, spectrum, market remedies, technical regulation, consumer protection and enforcement. [\[cite\]National Communications Act, 2012](#)[\[NCA official website\]](#)

3.2 **SUDESA.** SUDESA coordinates and implements neutral-host and publicly supported projects; structures PPPs under this Annex; and ensures contractual embedding of open-access obligations. [\[cite\]SUDESA framework \(EUSL package\)](#)

3.3 **DTSC.** The Digital Transformation Steering Committee adopts technical baselines, approves milestone plans and arbitrates inter-agency escalations within its mandate. [\[cite\]SUDESA governance texts](#)

3.4 **Hierarchy.** In case of conflict, statute and NCA regulations prevail; this Annex prevails over project-specific documents; specific licences/permits incorporate this Annex by reference unless expressly waived by NCA.

Article 4 — Open Access Obligations

4.1 **Passive Access.** Any passive infrastructure deployed (i) with public funds/incentives, or (ii) within public rights-of-way, or (iii) under SUDESA-coordinated PPPs, shall be made available on open, non-discriminatory terms pursuant to a Reference Offer approved by NCA. [\[cite\]ITU GSR Open Access Best-Practice](#)

4.2 **Active Wholesale.** Publicly supported NGA/NBN deployments shall offer a minimum wholesale product set (dark fibre, wavelength, bitstream and VULA) with published technical parameters to enable genuine service differentiation by access seekers. [\[cite\]EU Broadband Guidelines – model wholesale obligations](#)

4.3 **Non-Discrimination and Equivalence.** Access providers shall grant equivalence of input/output (EoI/EoO) and shall not engage in margin squeeze, undue preference, or information asymmetry.

4.4 **Functional/Structural Remedies.** Where significant market power persists, NCA may impose functional separation, and in exceptional cases structural separation or wholesale-only designation. [\[cite\]World Bank – separation and wholesale-only models](#)

Article 5 — Rights-of-Way, “Dig-Once”, and Civil Works Coordination

5.1 **One-Stop E-Permitting.** Competent authorities shall operate a one-stop, time-bound, electronic permitting process for civil works, with statutory decision periods and streamlined documentation. [\[cite\]BroadbandUSA: Policies & Mechanisms \(ROW/dig-once\)](#)

5.2 **Mandatory Multi-Duct/Dig-Once.** New or refurbished public roads and major excavations shall include multi-duct provision with spare capacity; micro-trenching may be mandated where safe and appropriate, subject to reinstatement standards. [\[cite\]BroadbandUSA ROW & micro-trenching guidance](#)

5.3 **Asset Registry.** A national registry of ducts, poles and fibre installed in public RoW shall be maintained, with FRAND access to as-built data for qualified operators under security safeguards.

Article 6 — Spectrum, 4G/5G Deployment and NTN Integration



6.1 Awards and Obligations. Spectrum awards shall be technology/service-neutral and may include coverage and performance obligations prioritising social infrastructure and rural areas. [cite][[World Bank – effective telecom markets & spectrum policy](#)]

6.2 Sharing and Refarming. NCA may authorise spectrum sharing/refarming consistent with efficient use, interference management and competitive neutrality.

6.3 5G System and Slicing. 5G deployments shall align with 3GPP system architecture, supporting network slicing, edge and small-cell neutral-host models in dense or high-cost zones. [cite][[3GPP 5G System Overview](#)]

6.4 NTN/Satellite. Satellite and NTN providers shall obtain landing rights, earth-station and terminal approvals, and integrate with terrestrial networks under wholesale frameworks; resilience/backhaul use-cases are encouraged. [cite][[3GPP 5G NTN references](#)]

Article 7 — Wholesale Products, SLAs and Reference Offers

7.1 Reference Offers. All access providers subject to Articles 4 and 5 shall publish an NCA-approved Reference Offer specifying access scope, technical parameters, ordering/provisioning/fault processes, and SLAs.

7.2 Minimum Product Set. The minimum set appears in **Schedule A** (dark fibre, wavelength, bitstream, VULA, Ethernet backhaul and passive elements).

7.3 SLAs and Transparency. SLA benchmarks for availability, MTTR, latency/jitter/packet loss, provisioning lead-times, and service credits shall comply with **Schedule B** and open-internet transparency practice. [cite][[BEREC Open-Internet Guidelines \(transparency/QoS\)](#)]

Article 8 — Pricing and Costing

8.1 Cost Orientation. Where effective competition is absent, NCA may impose cost-oriented wholesale prices based on LRIC(+) or alternative fit-for-purpose models, together with accounting separation.

8.2 Public Funding Conditionality. Publicly supported networks shall offer wholesale access on fair, transparent, and non-discriminatory terms; pricing shall reflect aid-minimisation and support multiple wholesale products (including VULA/bitstream/dark fibre). Model principles follow EU broadband state-aid guidance used internationally for open-access conditionality. [cite][[EU Guidelines on State Aid for Broadband Networks \(model reference\)](#)]

Article 9 — Interconnection, IXPs and Data Localisation

9.1 IXP Participation. Operators of significant scale shall peer at national IXPs on FRAND terms; SUDESA shall promote carrier-neutral colocation and regional peering to localise traffic and reduce transit costs. [cite][[Smart Africa initiatives on affordable broadband & continental backbone](#)]

9.2 Carrier-Neutral Facilities. New data-centre/colocation projects supported by SUDESA shall be carrier- and cloud-neutral with open interconnection policies to stimulate competition and local content hosting. [cite][[Smart Africa – data centre & backbone pillars](#)]

Article 10 — Universal Access, PPPs and Funding Instruments

10.1 Targeted Support. Where commercial viability is lacking, SUDESA may structure PPPs, viability-gap funding and blended finance conditioned on open-access obligations, verified coverage/quality targets and claw-backs. [cite][[World Bank – digital infrastructure, PPPs and gap financing](#)]



10.2 Roadmap Consistency. Measures shall align with the Broadband Commission/World Bank “Digital Infrastructure Moonshot for Africa” roadmap for universal, affordable, good-quality broadband. [\[cite\]Broadband Commission “Digital Moonshot for Africa”/World Bank report](#)

Article 11 — Open Internet and Traffic Management

11.1 Equal Treatment of Traffic. Internet access providers shall treat traffic equally subject only to transparent, necessary and proportionate traffic management; specialised services are permitted where they do not impair general IAS quality. Compliance is verified via certified monitoring mechanisms and public transparency. [\[cite\]BEREC Open-Internet Guidelines](#)

Article 12 — Mobile Infrastructure Sharing

12.1 Passive Sharing. Site, mast, power and backhaul sharing is generally permissible and encouraged, subject to safety and integrity of networks.

12.2 Active Sharing. Active RAN sharing (MOCN/MORAN) may be authorised by NCA with competition safeguards ensuring independent capacity and QoS. [\[cite\]GSMA Infrastructure Sharing Overview](#)

Article 13 — Monitoring, Dispute Resolution and Enforcement

13.1 Supervision. NCA shall approve and publish Reference Offers, monitor SLAs and wholesale KPIs, and enforce non-discrimination and equivalence.

13.2 Dispute Resolution. Wholesale disputes shall be resolved by NCA within statutory, expedited timelines; interim measures may be imposed to preserve service continuity.

13.3 Sanctions and Remedies. For breach, NCA may order specific performance, administrative fines, disgorgement of unlawful advantage, suspension of rights to publicly funded assets, or, in serious cases, recommend licence amendment/withdrawal pursuant to applicable law. [\[cite\]National Communications Act, 2012](#)

Article 14 — Regional and Continental Coordination

14.1 COMESA/Smart Africa Coordination. SUDESA and NCA shall support COMESA Digital Free Trade Area instruments and Smart Africa backbone, roaming and bulk-capacity initiatives to reduce costs and keep African traffic within Africa. [\[cite\]COMESA digital trade/DFTA materials](#) [Smart Africa initiatives](#)

Article 15 — Transitional Provisions, Amendments and Entry into Force

15.1 Transitional Application. Existing publicly supported networks shall file compliant Reference Offers within six (6) months of entry into force; NCA may grant justified extensions not exceeding a further six (6) months.

15.2 Amendments. The DTSC may propose technical amendments; NCA may adopt regulatory instruments to implement or refine this Annex after public consultation consistent with due process and regulatory independence. [\[cite\]TU–World Bank Digital Regulation \(regulatory governance\)](#)

15.3 Entry into Force. This Annex enters into force on the date specified in the SUDESA Instrument to which it is appended.

Schedule A — Minimum Wholesale Product Set (Normative)

A.1 Passive access to ducts, poles, towers, masts and associated civil works; site colocation and power.

A.2 Dark fibre (pair) on IRU/lease basis with standard splice/handover options.

A.3 Wavelength services ($\geq 10G$ and $\geq 100G$ classes) with defined OTN/Ethernet handover.

A.4 Layer-2/Layer-3 bitstream profiles with committed information rate and QoS classes.



A.5 VULA with local handover enabling multicast/IPv6 and access-seeker control of CPE profiles.

A.6 Ethernet backhaul from cell/sites and aggregation nodes. ^[2]^[3][EU Broadband Guidelines – wholesale products \(model reference\)](#)^[2][ITU GSR Open Access Best-Practice](#)^[2]

Schedule B — SLA Benchmarks and Transparency (Normative)

B.1 Availability targets per product class: ≥99.5% (standard), ≥99.9% (enhanced), ≥99.95% (mission-critical).

B.2 MTTR: urban ≤8 hours (standard) / ≤4 hours (enhanced); rural ≤24 hours unless otherwise agreed.

B.3 Latency/jitter/packet-loss envelopes appropriate to voice/video and business services (to be specified per class).

B.4 Provisioning lead-times: passive ≤30 days (subject to make-ready), bitstream/VULA ≤15 business days unless construction is required.

B.5 Service credits ladder for breach; planned-maintenance windows and notification obligations.

B.6 Public transparency: publication of parameters, certified measurement tools and complaint procedures consistent with open-internet guidance. ^[2]^[3][BEREC Open-Internet Guidelines – transparency and certified monitoring](#)^[2]

Schedule C — Rights-of-Way and Civil Works (Normative)

C.1 One-stop e-permitting; statutory response times; deemed consent in limited, defined circumstances; safety and reinstatement standards.

C.2 Multi-duct obligation with spare capacity; micro-trenching specifications and quality audits.

C.3 Publication of standard fees and templates; asset registry access for qualified operators under FRAND terms. ^[2]^[3][BroadbandUSA: ROW/dig-once guidance](#)^[2]

Schedule D — Spectrum, 5G and NTN (Normative)

D.1 Coverage obligations linked to schools, clinics and administrative facilities; verification via geospatial audits.

D.2 Support for neutral-host small-cell layers in dense venues and urban canyons; shared-infrastructure authorisations.

D.3 NTN/satellite landing rights; earth-station siting; terminal type approval; fair interconnection and backhaul integration. ^[2]^[3][3GPP 5G System/NTN overview](#)^[2]

Schedule E — Model PPP Clauses (Normative)

E.1 **Open-Access Covenant.** Concessionaire undertakes perpetual open-access obligations as per Articles 4, 7 and Schedules A–B; breach constitutes a material default.

E.2 **Tariff Regime.** Wholesale tariffs subject to NCA approval and periodic cost review; tariff glide-paths allowed with claw-backs where realised returns exceed agreed thresholds.

E.3 **Non-Discrimination & EoI.** Governance covenants to ensure equivalence (separate OSS/BSS access gateways; audit rights; independent compliance officer).

E.4 **Transparency.** Publication of KPIs, outages, capacity utilisation and ordering queues; equal information access for all access seekers.

E.5 **Step-In Rights.** Public step-in for critical service failure or persistent material breach, with orderly transition of operations. ^[2]^[3][World Bank – PPP & wholesale-only models](#)

Execution Clause

Executed as **Annex F** to the SUDESA Instruments on the date indicated therein. All Parties and Participants acknowledge and accept the legal obligations herein.



Notes on Authorities (non-exhaustive, for interpretive guidance)

- **African Union: *Digital Transformation Strategy for Africa (2020–2030)*** (continental policy anchor).
<https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>.
- **ITU/Digital Regulation (with World Bank):** Open access and regulatory governance guidance and case studies.
<https://www.itu.int/ITU-D/treg/>; <https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/DigiReg20.aspx>.
- **BEREC Open-Internet Guidelines** (transparency, QoS, monitoring frameworks).
https://www.berec.europa.eu/.../BoR_%2822%29_81_Update...pdf.
- **EU Broadband Guidelines** (model references for wholesale obligations in publicly funded networks).
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:4649196>.
- **World Bank/Broadband Commission: *Connecting Africa Through Broadband*** (Digital Moonshot).
<https://documents1.worldbank.org/.../Connecting-Africa-Through-Broadband.pdf>.
- **3GPP/ETSI:** 5G System/NTN integration references.
<https://www.3gpp.org/technologies/5g-system-overview>.
- **ROW and Dig-Once:** BroadbandUSA policy guidance.
<https://broadbandusa.ntia.gov/.../Broadband%20Policies%20Mechanisms%20PDF.pdf>.
- **Smart Africa/COMESA:** regional backbone, DFTA and digital trade facilitation.
<https://broadband.itu.int/smart-africa-initiatives/>; <https://www.comesa.int/.../CUSTOMS-DIGITALIZATION-...pdf>.

National Communication Authority (Open-Access Broadband) Regulation, 2025

(Model legal instrument to operationalise Articles 4–13 of Annex F—Open Access Broadband)

Part I — Preliminary

1. Citation and commencement.

This Regulation may be cited as the *National Communication Authority (Open-Access Broadband) Regulation, 2025* and shall come into force on the date specified in the Gazette notice issued by the National Communication Authority (“NCA”).

2. Legal basis.

This Regulation is made under Sections on licensing, interconnection, spectrum management, consumer protection and enforcement of the *National Communications Act, 2012* and any subsidiary instruments issued thereunder. It implements Articles 4–13 of *Annex F (Open Access Broadband — Technical and Regulatory Notes)* adopted under the SUDESA framework.

References: *National Communications Act, 2012* (text); NCA website for mandates.
[National Communications Act, 2012 \(official consolidated text\)](#) | [NCA – official site](#)

3. Objectives.

The objectives are:



- 3.1 to establish a binding open-access regime for passive and active wholesale broadband infrastructure and services;
- 3.2 to mandate wholesale product sets, Service Level Agreements (SLAs), transparency and non-discrimination;
- 3.3 to streamline rights-of-way (“RoW”) and “dig-once” processes;
- 3.4 to align spectrum awards, 5G/NTN integration and infrastructure sharing with open-access objectives;
- 3.5 to ensure open internet transparency and supervision; and
- 3.6 to provide monitoring, dispute-resolution and enforcement mechanisms.

References: ITU/Digital Regulation best practice on open access and regulatory governance; AU Digital Transformation Strategy.

[ITU GSR Open-Access Best-Practice](#) | [Digital Regulation Handbook/Platform \(ITU–World Bank\)](#) | [AU Digital Transformation Strategy 2020–2030](#)

4. Interpretation.

4.1 Terms defined in Annex F apply mutatis mutandis. In addition:

- (a) “Access Provider” means any Licensee controlling passive or active infrastructure subject to this Regulation.
- (b) “Reference Offer” means a published, NCA-approved wholesale offer compliant with this Regulation.
- (c) “Significant Market Power (SMP)” bears its ordinary meaning under competition and sectoral rules.

Part II — Scope and general duties

5. Scope of application.

This Regulation applies to: (a) any passive infrastructure located in public RoW; (b) any passive or active infrastructure built, upgraded, operated or maintained with public funds or fiscal incentives; (c) any SUDESA-coordinated PPP; and (d) any wholesale services designated by the NCA as essential or subject to SMP remedies.

6. General duties of Access Providers.

6.1 Access Providers shall provide open, transparent and non-discriminatory access to eligible wholesale seekers on terms no less favourable than those offered to their own retail divisions or affiliates (Equivalence of Input/Output).

6.2 Confidential information obtained from access seekers shall not be used for any competitive advantage or disclosed to retail divisions.

References: ITU open-access guidance; model wholesale non-discrimination/equivalence principles as used internationally.

[ITU GSR Open-Access Best-Practice](#)

Part III — Open access to passive and active infrastructure (Articles 4 & 7, Annex F)

7. Passive infrastructure access obligations.

7.1 Access Providers shall grant access to ducts, poles, towers, masts, handholes/manholes, shelters, power, and dark fibre, wherever such facilities are within public RoW or subject to public support.

7.2 Access shall include site surveys, make-ready works, capacity booking and standard colocation, subject to safety and engineering standards.

7.3 A Reference Offer for passive access shall be filed under Part V.



8. Active wholesale obligations.

8.1 Publicly supported NGA/NBN deployments shall provide, at minimum, the wholesale products listed in Schedule 1 (dark fibre, wavelength, Layer-2/Layer-3 bitstream profiles, VULA and Ethernet backhaul), with technical parameters enabling genuine service differentiation.

8.2 Access Providers with SMP may be required to supply additional ancillary services (e.g., multicast, IPv6, timing/sync) as necessary for equivalence.

References: Model wholesale product obligations and VULA/bitstream specifications used in open-access projects.

[Guidelines on State Aid for Broadband Networks \(model reference\)](#)

Part IV — Rights-of-way and civil-works coordination (Article 5, Annex F)

9. One-stop e-permitting and statutory timelines.

9.1 The NCA, in concert with competent authorities, shall operate a one-stop electronic permitting portal for telecom civil works.

9.2 Decisions on complete applications shall be issued within 30 working days for routine permits and 60 working days for complex works; reasons shall accompany any refusal.

9.3 Expedited treatment (≤ 15 working days) shall apply to minimally invasive techniques meeting standards in Schedule 3.

References: International best practice on RoW streamlining, micro-trenching and one-stop shops.

[BroadbandUSA – RoW, dig-once, OTMR guidance](#)

10. “Dig-once” and multi-duct.

10.1 All new or refurbished public roads and utility corridors shall incorporate multi-ducts with spare capacity for third-party access.

10.2 Micro-trenching may be mandated where safe and appropriate; reinstatement and quality audits follow Schedule 3.

References: As above (RoW/dig-once).

[BroadbandUSA – Policies & Mechanisms](#)

Part V — Reference Offers, product catalogues and SLAs (Articles 7 & 8, Annex F)

11. Filing and approval.

11.1 Each Access Provider subject to Parts II–IV shall file a Reference Offer (passive and/or active, as applicable) within 90 calendar days of this Regulation’s commencement, or within 60 days of project handover for new publicly supported builds.

11.2 The NCA shall review completeness within 15 working days and approve, modify or reject the filing within 60 working days; silence beyond 60 working days shall not constitute approval.

12. Mandatory contents.

12.1 The Reference Offer shall include: (a) product descriptions and technical specifications; (b) ordering/provisioning, migration and fault-handling processes; (c) handover points; (d) KPIs and SLAs; (e) price lists and price-control methodology where applicable; and (f) template agreements.

Minimum content is set out in Schedule 2.

13. Publication and change control.

13.1 The Access Provider shall publish the approved Reference Offer on its website within ten (10) working days of approval.

13.2 Material changes require prior NCA approval; minor editorial changes must be notified within five (5) working days.

14. SLAs and quality.

14.1 SLAs shall at least meet Schedule 4 benchmarks (availability, MTTR, latency/jitter/packet-loss, provisioning lead times, service credits).

14.2 Transparency, reporting and monitoring shall follow open internet transparency guidance and certified measurement mechanisms.

References: Open internet transparency and certified monitoring frameworks adopted by regulators.
[BEREC Open-Internet Guidelines](#)

Part VI — Pricing, cost orientation and accounting separation (Article 9, Annex F)

15. Price control.

15.1 Where the NCA determines that effective competition is absent, it may impose cost-oriented prices based on LRIC(+) or another fit-for-purpose model, including retail-minus where justified.

15.2 Volume discounts and promotional terms must be non-discriminatory and transparently published.

16. Accounting separation and audits.

16.1 Access Providers with SMP shall implement accounting separation within nine (9) months and submit annual statements for independent audit.

16.2 The NCA may require cost models, usage factors, and reconciliation with Reference Offer price lists.

References: International frameworks for wholesale price control and separation in open-access/state-supported networks.

[Guidelines on State Aid for Broadband Networks \(model reference\)](#) | [Digital Regulation Handbook \(pricing/separation\)](#)

Part VII — Interconnection, IXPs and data-centre neutrality (Article 10, Annex F)

17. IXP participation and peering.

17.1 Operators above thresholds set by the NCA shall establish settlement-free peering at designated national IXPs on fair, reasonable and non-discriminatory (FRAND) terms, subject to reasonable technical policies.

17.2 SUDESA-supported data centres shall operate on a carrier- and cloud-neutral basis with open interconnection policies to localise traffic and reduce transit costs.

References: Regional initiatives to keep African traffic in-region and reduce costs; continental backbone and data-centre thrusts.

[Smart Africa – broadband affordability & backbone/Data Centre pillars](#)

Part VIII — Spectrum, 5G and NTN integration (Article 6, Annex F)

18. Awards and obligations.

18.1 Spectrum awards shall be technology- and service-neutral and may include coverage/quality obligations prioritising schools, clinics and administrative sites, verified by geospatial audits.

18.2 The NCA may authorise spectrum sharing/refarming consistent with efficient use and competitive neutrality.

19. 5G and NTN.

19.1 5G deployments shall align to 3GPP 5G System architecture and support, where required, neutral-host small-cell layers.

19.2 Satellite/NTN service providers shall obtain landing rights, earth-station and terminal approvals; interworking with terrestrial networks is encouraged for resilience.

References: 3GPP 5G system and NTN integration baseline; World Bank guidance on effective telecom markets.

[3GPP 5G System Overview](#) | [World Bank – Digital Infrastructure overview](#)

Part IX — Open Internet supervision (Article 12, Annex F)

20. Equal treatment of traffic and transparency.

20.1 Internet access providers shall treat traffic equally, subject only to transparent, necessary and proportionate traffic-management.

20.2 Specialised services may be offered provided they do not impair the general quality of internet access services.

20.3 The NCA shall certify monitoring tools, require publication of speeds/QoS and provide complaint procedures.

References: Supervisory frameworks and transparency requirements.

[BEREC Open-Internet Guidelines](#)

Part X — Mobile infrastructure sharing (Article 12, Annex F)

21. Passive and active sharing.

21.1 Passive sharing (sites, masts, power, backhaul) is permitted and encouraged, subject to safety and network integrity.

21.2 Active sharing (MORAN/MOCN/RAN sharing) may be authorised with safeguards ensuring independent capacity, QoS, spectrum use transparency and competition compliance.

References: GSMA/industry and regulatory best-practice on passive/active sharing.

[GSMA – Infrastructure Sharing: Overview](#)

Part XI — Monitoring, reporting and audits

22. KPI reporting.

22.1 Access Providers shall submit quarterly KPI reports (ordering queues, provisioning lead times, availability, MTTR, latency/jitter/packet-loss, utilisation of ducts/poles/fibre, dispute volumes) in the format prescribed in Schedule 5.

22.2 The NCA shall publish an annual Open-Access Scorecard.

23. Independent audits and inspections.

23.1 The NCA may commission technical/financial audits and conduct on-site inspections with reasonable notice; urgent inspections may be unannounced where public interest so requires.

References: ITU/World Bank regulatory governance – supervision and transparency.

[Digital Regulation Handbook/Platform](#)

Part XII — Dispute resolution

24. Procedure and timelines.

24.1 Parties shall first attempt negotiation for up to ten (10) working days.

24.2 A dispute may then be filed with the NCA using the standard form in Schedule 6; the responding party shall answer within ten (10) working days.

24.3 The NCA shall determine the dispute within forty-five (45) working days of a complete filing; interim measures may be imposed to ensure service continuity.

References: Time-bound regulatory dispute processes reflected in sectoral best practice.

[Digital Regulation Handbook/Platform](#)



Part XIII — Enforcement, sanctions and remedies

25. Sanctions.

25.1 For breach, the NCA may impose administrative fines proportionate to gravity and duration, order specific performance, mandate refunds/service credits, require structural or functional remedies, suspend access to publicly funded assets, or recommend licence variation/withdrawal in accordance with the *National Communications Act, 2012*.

References: Statutory enforcement powers and proportionate remedies.

[National Communications Act, 2012](#)

26. Claw-backs and public-funding safeguards.

26.1 Where realised returns materially exceed approved thresholds in publicly supported projects, the NCA may order claw-backs and tariff revisions to restore affordability and competitive neutrality.

References: Model safeguards from state-supported broadband frameworks.

[Guidelines on State Aid for Broadband Networks \(model reference\)](#)

Part XIV — Transitional and final provisions

27. Transitional filing.

27.1 Existing Access Providers subject to Parts II–IV shall file Reference Offers within six (6) months of commencement.

27.2 The NCA may grant a single extension not exceeding six (6) months upon reasoned request.

28. Amendments.

28.1 The NCA may issue determinations, guidelines and forms to implement this Regulation following public consultation proportionate to the subject matter.

References: Good-regulation principles for consultation and iterative guidance.

[Digital Regulation Handbook/Platform](#)

29. Entry into force.

29.1 This Regulation enters into force on the date specified in the Gazette.

Schedules (Normative)

Schedule 1 — Minimum Wholesale Product Set (Article 8)

1. Passive access: ducts, poles, towers, site colocation and power; make-ready and capacity booking.
2. Dark fibre (pair) on IRU/lease basis; splice points and handover.
3. Wavelength services ($\geq 10\text{G}$ and $\geq 100\text{G}$ classes) with OTN/Ethernet handover.
4. Layer-2/Layer-3 bitstream profiles with CIR, QoS classes, multicast, IPv6.
5. VULA with local handover and access-seeker control of CPE profiles.
6. Ethernet backhaul for cell/sites and aggregation nodes.

Reference: [EU Broadband Guidelines – wholesale products \(model reference\)](#)

Schedule 2 — Reference Offer minimum content (Articles 11–13)

1. Product catalogue and technical specifications; 2. eligibility and ordering; 3. provisioning/migration; 4. fault handling (targets and escalation); 5. interfaces and handover;



6. KPIs/SLAs and service credits; 7. price list and price-control methodology; 8. template agreement; 9. change-control; 10. data-protection and security.

Schedule 3 — RoW & Civil-Works Standards (Articles 9–10)

1. One-stop e-permit forms and required drawings; 2. statutory decision timelines; 3. micro-trenching specifications (depth/width, materials, reinstatement); 4. safety and traffic-management measures; 5. multi-duct design (dimensioning and spare capacity); 6. quality audits and remediation.

Reference: [BroadbandUSA – Policies & Mechanisms](#)

Schedule 4 — SLA Benchmarks (Article 14)

1. Availability: Standard $\geq 99.5\%$; Enhanced $\geq 99.9\%$; Mission-critical $\geq 99.95\%$.
2. MTTR: Urban $\leq 8h$ (standard)/ $\leq 4h$ (enhanced); Rural $\leq 24h$ unless otherwise agreed.
3. Latency/jitter/packet-loss envelopes per product class; 4. provisioning lead-times: passive ≤ 30 days (subject to make-ready); bitstream/VULA ≤ 15 business days unless construction is required; 5. service-credit ladder; 6. planned-maintenance notification.

Reference: [BEREC Open-Internet Guidelines – transparency & certified monitoring](#)

Schedule 5 — KPI Reporting Schema (Article 22)

Quarterly dataset at service/region granularity: orders received/accepted/rejected and reasons; average/95th-percentile provisioning times; availability and MTTR; latency/jitter/loss; utilisation (ducts, fibre, ports); outages (planned/unplanned); wholesale seeker complaint volumes and resolution times.

Schedule 6 — Dispute Form and Procedure (Article 24)

Standardised form including: parties' details; product/service in dispute; chronology; attempted settlement; relief sought; annexes (correspondence, logs, measurements). Filing via the NCA portal; service on respondent by portal notification and email; status tracking; interim-measures request.

Explanatory Note (non-normative)

This model Regulation translates Annex F's policy baselines into enforceable obligations and processes. It draws upon (i) AU continental strategy for a Digital Single Market; (ii) ITU/Digital Regulation guidance on open-access, governance and dispute processes; (iii) model wholesale obligations from the EU broadband state-aid framework for publicly supported networks; (iv) BEREC open-internet transparency and supervision; (v) 3GPP 5G/NTN architecture for technology neutrality and neutral-host options; (vi) BroadbandUSA RoW/dig-once practice; and (vii) Smart Africa initiatives on backbone, data-centre neutrality and in-continent traffic localisation.

Key references:

[AU Digital Transformation Strategy 2020–2030](#) | [ITU GSR Open-Access Best-Practice](#) | [Digital Regulation Handbook/Platform](#) | [EU Broadband Guidelines – model reference](#) | [BEREC Open-Internet Guidelines](#) | [3GPP 5G System Overview](#) | [BroadbandUSA – RoW/dig-once](#) | [Smart Africa – broadband initiatives](#)

Annex H: Risk Register Template and Guidance

H.1 Purpose and Scope

This annex provides a standardised framework for identifying, assessing, and monitoring risks associated with the implementation of the SUDESA Mission. It ensures that all stakeholders adopt a consistent approach to risk management, aligned with international best practices such as ISO 31000:2018 Risk Management Guidelines (<https://www.iso.org/standard/65694.html>) and the World Bank Environmental and Social Framework (ESF) (<https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>).

The Risk Register serves as a living document, updated quarterly or upon the occurrence of significant events, and forms part of the Monitoring, Evaluation, and Learning (MEL) system described in Annex G.

H.2 Risk Management Principles

The risk management process shall adhere to the following principles:

1. **Integration:** Risk management is embedded in all planning, procurement, and operational processes.
2. **Transparency:** Risks and mitigation measures are documented and disclosed to relevant governance bodies.
3. **Proportionality:** Risk treatment measures are commensurate with the severity and likelihood of the identified risk.
4. **Accountability:** Risk ownership is clearly assigned to responsible entities within the governance structure.

H.3 Risk Categories

Risks shall be classified under the following categories:

- **Strategic Risks:** Risks affecting the achievement of mission objectives, including political instability and policy reversals.
- **Operational Risks:** Risks arising from internal processes, systems, and human resources.
- **Financial Risks:** Risks related to funding shortfalls, currency volatility, and fiduciary non-compliance.
- **Legal and Regulatory Risks:** Risks associated with delays in enacting enabling legislation or non-compliance with international standards.
- **Technological Risks:** Risks linked to system failures, cybersecurity breaches, and obsolescence.
- **Environmental and Social Risks:** Risks impacting communities, ecosystems, and social inclusion objectives.

H.4 Risk Assessment Methodology

Each risk shall be assessed using a **5x5 matrix** based on:

- **Likelihood:** Rated from 1 (Rare) to 5 (Almost Certain).
- **Impact:** Rated from 1 (Insignificant) to 5 (Catastrophic).



The **Risk Rating** is calculated as *Likelihood* $\times$ *Impact*, producing a score between 1 and 25. Risks are categorised as:

- **Low (1–5):** Monitor.
- **Moderate (6–10):** Mitigate with standard controls.
- **High (11–15):** Escalate to governance committees.
- **Critical (16–25):** Immediate action and contingency planning.



H.5 Risk Register Template

Risk ID	Risk Description	Category	Likelihood (1–5)	Impact (1–5)	Risk Rating	Mitigation Measures	Residual Risk	Owner	Review Date
R-001	Delay in enactment of Data Protection Act	Legal/Regulatory	4	4	16 (Critical)	Fast-track legislative drafting; Presidential Directive; interim compliance guidelines	Moderate	Ministry of Justice	Q2 2026
R-002	Cybersecurity breach in e-Government platform	Technological	3	5	15 (High)	Zero Trust architecture; ISO 27001 certification; CERT activation	Low	DTSC/National CERT	Q1 2026

H.6 Reporting and Escalation

- **Quarterly Risk Reports** shall be submitted to the **Digital Transformation Steering Committee (DTSC)** and the **Joint Steering Committee (JSC)**.
- **Critical Risks** (score ≥ 16) must be escalated within 48 hours to the JSC and, where necessary, to the Office of the President.
- Risk mitigation progress shall be tracked through the MEL system and linked to performance indicators in Annex G.

H.7 References

- **ISO 31000:2018 Risk Management Guidelines:** <https://www.iso.org/standard/65694.html>
- **World Bank Environmental and Social Framework (ESF):**
<https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>
- **African Development Bank Integrated Safeguards System (ISS):**
<https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>

Sample Risk Register (Illustrative)

Risk ID	Risk Description	Category	Likelihood (1–5)	Impact (1–5)	Risk Rating	Mitigation Measures	Residual Risk	Owner	Review Date
R-001	Delay in enactment of Data Protection & Privacy Act	Legal/Regulatory	4	4	16 (Critical)	Fast-track drafting; Presidential Directive; interim compliance guidelines	Moderate	Ministry of Justice	Q2 2026
R-002	Cybersecurity breach in e-Government platform	Technological	3	5	15 (High)	Zero Trust architecture; ISO 27001 certification; CERT activation	Low	DTSC/National CERT	Q1 2026
R-003	Political instability disrupting	Strategic	3	5	15 (High)	Stakeholder engagement; contingency planning;	Moderate	Office of the President	Continuous



Risk ID	Risk Description	Category	Likelihood (1–5)	Impact (1–5)	Risk Rating	Mitigation Measures	Residual Risk	Owner	Review Date
	implementation					phased rollouts			
R-004	Funding shortfall for DTIF commitments	Financial	3	4	12 (High)	Blended finance; donor coordination; phased disbursement	Moderate	Ministry of Finance/DTIF Board	Q3 2026
R-005	Vendor lock-in due to proprietary solutions	Technological	2	4	8 (Moderate)	Open standards mandate; interoperability testing; multi-vendor procurement	Low	DTSC	Q2 2026
R-006	Low digital literacy among civil servants	Operational	4	3	12 (High)	Mandatory training; certification programs; e-learning platforms	Moderate	Civil Service Commission	Q4 2026
R-007	Social exclusion of vulnerable groups in digital rollout	Social	3	4	12 (High)	Accessibility standards; targeted outreach; inclusive design	Low	Ministry of Gender & Social Welfare	Q3 2026
R-008	Delays in broadband infrastructure deployment	Operational	3	4	12 (High)	One-stop RoW permitting; dig-once policy; PPP acceleration	Moderate	NCA/SUEDSA	Q2 2026



Risk ID	Risk Description	Category	Likelihood (1–5)	Impact (1–5)	Risk Rating	Mitigation Measures	Residual Risk	Owner	Review Date
R-009	Non-compliance with environmental safeguards	Environmental	2	4	8 (Moderate)	ESIA compliance; AfDB ISS and World Bank ESF adherence; independent audits	Low	Ministry of Environment	Q3 2026
R-010	Currency volatility impacting procurement costs	Financial	3	3	9 (Moderate)	Hedging strategies; local currency contracts; contingency reserves	Moderate	Ministry of Finance	Q2 2026
R-011	Data localisation disputes with cloud providers	Legal/Technological	2	4	8 (Moderate)	Sovereign cloud agreements; hybrid hosting; contractual safeguards	Low	DTSC/NCA	Q3 2026
R-012	Reputational risk from project delays or failures	Strategic	3	4	12 (High)	Transparent reporting; proactive communication; escalation protocols	Moderate	SUDESA/JSC	Continuous

Key Notes

- **Critical Risks (≥16):** Immediate escalation to JSC and Office of the President.
- **High Risks (11–15):** Require detailed mitigation plans and monthly monitoring.
- **Moderate Risks (6–10):** Managed through standard controls and quarterly review.
- **Low Risks (≤5):** Monitor and report in quarterly updates.

Annex I: Communications and Disclosure Protocols

I.1 Purpose and Scope

This annex establishes the mandatory protocols for internal and external communications, disclosure of information, and stakeholder engagement under the SUDESA Mission. It ensures that all communications are accurate, timely, and compliant with applicable legal, fiduciary, and governance standards, including the African Union Digital Transformation Strategy, the World Bank Environmental and Social Framework (ESF), and the AfDB Integrated Safeguards System (ISS).

The protocols apply to all entities operating under the SUDESA framework, including government ministries, agencies, development partners, and private sector participants.

I.2 Guiding Principles

Communications and disclosure activities shall adhere to the following principles:

- **Transparency:** All material information related to program objectives, progress, and risks shall be disclosed to relevant stakeholders in a timely and accessible manner.
- **Accuracy:** Information disseminated must be factually correct, verified, and consistent with official records.
- **Confidentiality:** Sensitive data, including personal information and commercially confidential material, shall be protected in accordance with the **Data Protection and Privacy Act** and international standards such as the **Malabo Convention** (<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>).
- **Inclusivity:** Communications shall be accessible to all stakeholders, including persons with disabilities and those in rural or underserved areas, through multilingual and multi-channel dissemination.

I.3 Internal Communication Protocols

All internal communications between SUDESA, the Digital Transformation Steering Committee (DTSC), and the Joint Steering Committee (JSC) shall be conducted through secure, encrypted channels using enterprise-grade platforms such as **Microsoft 365 Government Suite** and **Teams**. Meeting agendas, minutes, and decisions shall be recorded in the official document management system and classified according to the Information Security Policy.

Critical decisions, risk escalations, and compliance alerts must be communicated within 24 hours to the relevant governance body. Internal reports shall follow the standard templates provided in Annex G (MEL Indicator Catalogue) and Annex H (Risk Register).

I.4 External Communication and Public Disclosure

External communications, including press releases, policy briefs, and stakeholder updates, shall be coordinated by the **SUDESA Communications Unit** under the supervision of the JSC. All public disclosures must:

- Be approved by the JSC or its delegated authority.
- Include clear references to the SUDESA Mission, Agenda for Social Equity 2074, and relevant legal frameworks.
- Avoid speculative statements or commitments not formally endorsed by the governance structure.



Public disclosure of procurement data shall comply with the **Open Contracting Data Standard (OCDS)** (<https://standard.open-contracting.org/latest/en/>) and be published on the official SUDESA portal within 10 working days of contract award.

I.5 Stakeholder Engagement and Consultation

Stakeholder consultations shall be conducted at key stages of program design, implementation, and evaluation. Engagement activities must:

- Follow the World Bank ESF (<https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>) and AfDB ISS <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539> .
- Ensure representation of vulnerable groups, including women, youth, and persons with disabilities.
- Document feedback and integrate it into decision-making processes, with a summary report published on the official portal.

I.6 Crisis Communication and Incident Reporting

In the event of a cybersecurity breach, data loss, or other critical incident, the following steps shall apply:

1. Immediate notification to the DTSC and National CERT within two hours of detection.
2. Preliminary incident report submitted within 24 hours, including nature, scope, and initial containment measures.
3. Public disclosure, where required, within 72 hours, in compliance with the Data Protection and Privacy Act and international norms such as GDPR.

I.7 Monitoring and Compliance

Compliance with these protocols shall be monitored through quarterly audits conducted by the SUDESA Internal Audit Unit and verified by independent evaluators under the MEL framework. Non-compliance may result in administrative sanctions, including suspension of communication privileges or contractual penalties for private sector partners.

References

- **African Union Digital Transformation Strategy (2020–2030):**
<https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>
- **Malabo Convention on Cyber Security and Personal Data Protection:**
<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>
- **Open Contracting Data Standard (OCDS):** <https://standard.open-contracting.org/latest/en/>
- **World Bank Environmental and Social Framework (ESF):**
<https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>



- **AfDB Integrated Safeguards System (ISS):** <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>

Annex I – Communications Matrix

Audience	Information Type	Channel(s)	Frequency	Responsible Party
Office of the President	Strategic updates, risk escalations, policy directives	Secure briefing notes, encrypted email, in-person briefings	Monthly or as required for critical issues	JSC Chair / SUDESA Executive Director
Joint Steering Committee (JSC)	Program performance, financial reports, compliance updates	Microsoft Teams, official portal, quarterly reports	Quarterly and ad hoc	SUDESA Secretariat
Digital Transformation Steering Committee (DTSC)	Technical progress, architecture compliance, cybersecurity alerts	Teams, secure dashboards, incident reports	Bi-weekly and immediate for incidents	DTSC Technical Lead
Development Partners (AfDB, World Bank, Nordic DFIs)	Financial disbursement status, safeguards compliance, MEL indicators	Official portal, donor coordination meetings, OCDS-compliant disclosures	Quarterly and upon milestone completion	DTIF Secretariat
Government Ministries & Agencies	Implementation guidelines, capacity-building schedules	Circulars, Teams, official portal	Monthly	SUDESA Program Coordination Unit
Private Sector Vendors & PPP Partners	Procurement notices, compliance requirements, SLA performance	Official portal, email notifications, OCDS publication	As per procurement cycle	SUDESA Procurement Unit
Civil Society & Advocacy Groups	Social inclusion updates, stakeholder consultation outcomes	Public portal, press releases, community forums	Semi-annual	SUDESA Communications Unit
General Public	Program milestones, broadband rollout updates, citizen services	Official website, social media, press releases, radio	Quarterly and milestone-based	SUDESA Communications Unit



Audience	Information Type	Channel(s)	Frequency	Responsible Party
Media Outlets	Press briefings, official statements, crisis communication	Press conferences, media kits, verified social channels	As needed	SUDESA Communications Unit
Regulatory Authorities (NCA, Data Protection Authority)	Compliance reports, audit findings, enforcement actions	Secure portal, formal submissions	Quarterly and ad hoc	SUDESA Compliance Office

Key Compliance References

- Open Contracting Data Standard (OCDS) for procurement transparency: <https://standard.open-contracting.org/latest/en/>
- World Bank ESF for stakeholder engagement: <https://documents.worldbank.org/en/projects-operations/environmental-and-social-framework>
- AfDB ISS for disclosure obligations: <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>

Annex J: Device Specification and Lifecycle Policy

J.1 Purpose and Scope

This annex defines the technical specifications, security requirements, and lifecycle management policies for all end-user devices deployed under the SUDESA Mission. It ensures that devices used by civil servants, educators, and community access points meet international standards for performance, security, and sustainability. The policy aligns with **ISO/IEC 27001** for information security management (<https://www.iso.org/standard/27001>) and the **African Union Digital Transformation Strategy (2020–2030)** (<https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>).

J.2 Device Categories

Devices covered by this policy include:

- **Government-issued laptops and tablets** for civil servants and educators.
- **Student learning devices** for digital education programs.
- **Community access devices** for public digital hubs and e-service kiosks.

J.3 Minimum Technical Specifications

All devices shall meet or exceed the following baseline specifications:

- **Processor:** Quad-core, 2.0 GHz or higher (Intel i5 equivalent or ARM-based for tablets).
- **Memory:** Minimum 8 GB RAM for laptops; 4 GB for tablets.
- **Storage:** 256 GB SSD for laptops; 64 GB for tablets (expandable).
- **Display:** Minimum 12-inch for laptops; 10-inch for tablets; HD resolution.
- **Connectivity:** Wi-Fi 6, Bluetooth 5.0, and LTE/5G capability for mobile devices.
- **Battery Life:** Minimum 8 hours under normal usage.
- **Operating System:** Windows 11 Enterprise (for laptops) or Android 13+ (for tablets), with enterprise-grade security features.
- **Security Features:** TPM 2.0, Secure Boot, BitLocker encryption, biometric authentication (fingerprint or facial recognition).
- **Accessibility:** Compliance with **WCAG 2.1** standards for assistive technologies (<https://www.w3.org/TR/WCAG21/>).

J.4 Security and Compliance Requirements

- All devices must be enrolled in **Microsoft Intune** for Mobile Device Management (MDM) and compliance monitoring.
- Mandatory installation of **Microsoft Defender for Endpoint** and configuration of **Zero Trust security policies**.
- Devices must support **multi-factor authentication (MFA)** and enforce password complexity standards.
- Regular security patching and firmware updates shall be automated through the central management system.



J.5 Lifecycle Management

The lifecycle policy includes:

- **Procurement:** Devices shall be procured through transparent, OCDS-compliant processes (<https://standard.open-contracting.org/latest/en/>).
- **Deployment:** Devices will be pre-configured with enterprise security profiles and user-specific access rights.
- **Maintenance:** Preventive maintenance schedules and remote diagnostics will be implemented.
- **Replacement Cycle:** Standard replacement every 4 years for laptops and 3 years for tablets, subject to performance audits.
- **Decommissioning:** Devices reaching end-of-life shall undergo certified data wiping in compliance with **NIST SP 800-88** guidelines (<https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>) and environmentally responsible disposal in line with **ISO 14001** environmental standards (<https://www.iso.org/iso-14001-environmental-management.html>).

J.6 Sustainability and Circular Economy

- Devices shall be sourced from manufacturers adhering to **EPEAT** and **Energy Star** certifications for energy efficiency.
- Refurbishment and redeployment programs will be implemented for devices in good condition.
- E-waste recycling partnerships shall be established with certified vendors to ensure compliance with environmental regulations.

References

- **ISO/IEC 27001 Information Security Management:** <https://www.iso.org/standard/27001>
- **NIST SP 800-88 Media Sanitization Guidelines:** <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>
- **ISO 14001 Environmental Management:** <https://www.iso.org/iso-14001-environmental-management.html>
- **WCAG 2.1 Accessibility Standards:** <https://www.w3.org/TR/WCAG21/>
- **Open Contracting Data Standard (OCDS):** <https://standard.open-contracting.org/latest/en/>

Annex K: Accessibility and Inclusion Standards (Education)

K.1 Purpose and Scope

This annex establishes the mandatory accessibility and inclusion standards for all digital education initiatives under the SUDESA Mission. It ensures that educational platforms, content, and delivery mechanisms are inclusive, equitable, and compliant with international norms such as the **Web Content Accessibility Guidelines (WCAG) 2.1** (<https://www.w3.org/TR/WCAG21/>), the **UN Convention on the Rights of Persons with Disabilities (CRPD)**

<https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html>

K.2 Guiding Principles

The accessibility and inclusion framework is based on the following principles:

- **Universal Design for Learning (UDL):** Educational content and platforms must accommodate diverse learning needs and preferences.
- **Equity and Non-Discrimination:** No learner shall be excluded on the basis of disability, gender, language, or socio-economic status.
- **Technology as an Enabler:** Digital tools must reduce—not reinforce—existing barriers to education.

K.3 Digital Platform Accessibility Standards

All e-learning platforms and digital education tools shall:

- Comply with **WCAG 2.1 Level AA** standards for web accessibility <https://www.w3.org/TR/WCAG21/>.
- Provide **text-to-speech** and **speech-to-text** functionality for visually and hearing-impaired learners.
- Include **keyboard navigation** and **screen reader compatibility** for all interactive elements.
- Offer **adjustable font sizes**, **high-contrast modes**, and **color-blind friendly palettes**.
- Support **multilingual interfaces**, including English, Arabic, and major local languages.

K.4 Inclusive Content Design

Educational content must:

- Be available in **multiple formats** (text, audio, video, and interactive simulations).
- Include **closed captions** and **sign language interpretation** for video content.
- Provide **alternative text descriptions** for all images and graphics.
- Ensure that assessments are accessible, with accommodations for learners with disabilities.

K.5 Assistive Technologies and Device Integration

- All government-issued devices (as per Annex J) must support assistive technologies such as **screen readers**, **Braille displays**, and **voice recognition software**.



- Schools and community learning hubs shall be equipped with adaptive hardware (e.g., alternative keyboards, hearing aids) where required.
- Partnerships with global technology providers will ensure integration of accessibility features into core learning platforms.

K.6 Teacher Training and Capacity Building

- Teacher training programs shall include modules on inclusive pedagogy, digital accessibility, and assistive technology use.
- Certification programs will be developed in collaboration with universities and teacher training institutes to ensure sustainability.

K.7 Monitoring and Compliance

- Compliance with accessibility standards will be assessed through **annual audits** conducted by the SUDESA Education Division in collaboration with the Ministry of General Education and Instruction.
- Non-compliance will trigger corrective action plans and may affect eligibility for funding under the Digital Education Program.

References

- **WCAG 2.1 Accessibility Standards:** <https://www.w3.org/TR/WCAG21/>
- **UN CRPD:** <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html>
- **African Union CESA 16-25:** <https://au.int/en/cesa>
- **ISO/IEC 40500:2012 (WCAG 2.0):** <https://www.iso.org/standard/58625.html>

Annex K – Accessibility Compliance Checklist

Section 1: Digital Platform Accessibility

- Platform complies with WCAG 2.1 Level AA standards (<https://www.w3.org/TR/WCAG21/>).
- All interactive elements are keyboard navigable and screen reader compatible.
- Platform supports text-to-speech and speech-to-text functionality.
- Adjustable font sizes, high-contrast mode, and color-blind friendly palettes are available.
- Multilingual interface implemented (English, Arabic, and major local languages).

Section 2: Inclusive Content Design

- All video content includes closed captions and sign language interpretation.
- Alternative text descriptions provided for all images and graphics.
- Educational materials available in multiple formats (text, audio, video, interactive).
- Assessments designed with accommodations for learners with disabilities.

Section 3: Device Accessibility

- All devices support assistive technologies (screen readers, Braille displays, voice recognition).
- Accessibility features pre-configured during deployment (as per Annex J).



- Devices comply with WCAG 2.1 and ISO/IEC 40500:2012 standards (<https://www.iso.org/standard/58625.html>).

Section 4: Teacher Training and Capacity Building

- Teacher training includes modules on **inclusive pedagogy** and **digital accessibility**.
- Training covers use of **assistive technologies** and accessible content creation.
- Certification programs established for teachers on accessibility compliance.

Section 5: Monitoring and Reporting

- Annual accessibility audits conducted by SUDESA Education Division.
- Compliance reports submitted to the **Digital Transformation Steering Committee (DTSC)**.
- Corrective action plans implemented for non-compliance.

References

- **WCAG 2.1 Accessibility Standards:** <https://www.w3.org/TR/WCAG21/>
- **UN CRPD:** <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html>
- **ISO/IEC 40500:2012 (WCAG 2.0):** <https://www.iso.org/standard/58625.html>