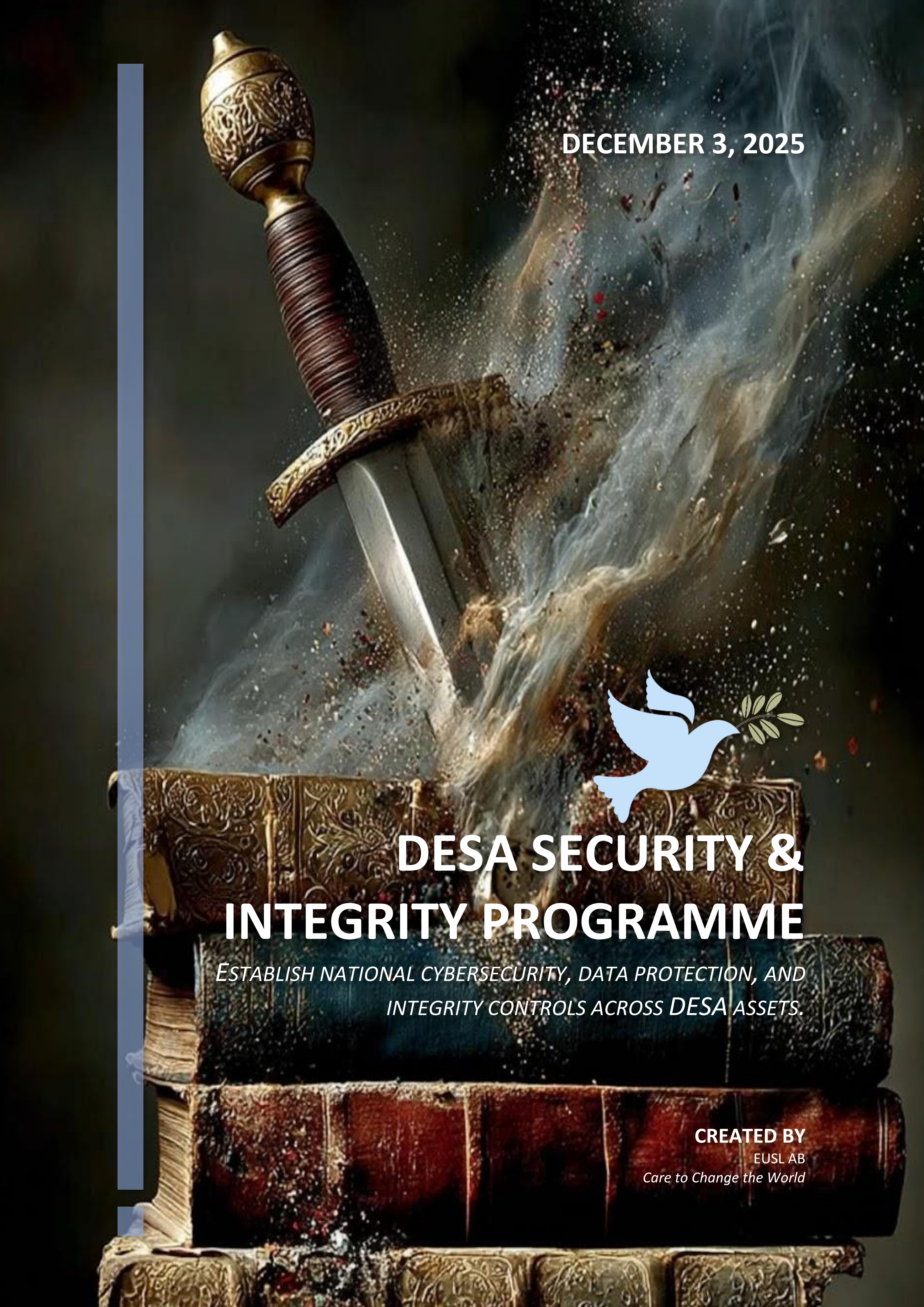

DECEMBER 3, 2025

DESA SECURITY & INTEGRITY PROGRAMME

ESTABLISH NATIONAL CYBERSECURITY, DATA PROTECTION, AND INTEGRITY CONTROLS ACROSS DESA ASSETS.

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

DESA Security & Integrity Program

Chapter 1. Programme Title and Acronym

The Programme shall be known as the **DESA Security & Integrity Program**, referenced by the acronym **DSIP**. Its short title line is defined as follows:

Mandate: *Establish national cybersecurity, data protection, and integrity controls across DESA assets.*
Scope: *Zero Trust architectures, national Computer Emergency Response Team (CERT), threat detection, incident response, privacy by design, and staff cyber hygiene certification.*
Instruments: *Legal instruments aligned with Malabo Convention principles, Security Operations Center (SOC) capabilities, red team exercises, and breach notification standards.*
Intended Outcomes: *Shorter incident response times, lower successful attack rates, and demonstrable compliance with data governance obligations.*

Table 1 — Programme Header

Field	Entry
Programme Name	DESA Security & Integrity Program
Acronym	DSIP
One-Line Mission	Establish national cybersecurity, data protection, and integrity controls across DESA assets.
Scope	Zero Trust architectures; national CERT; threat detection; incident response; privacy by design; staff cyber hygiene certification.
Principal Instruments	Malabo-aligned legal instruments; SOC capabilities; red team exercises; breach notification standards.
Intended Outcomes	Reduced incident response times; lower attack success rates; demonstrable compliance with data governance.

Chapter 2. Legal Mandate and Purpose

2.1. Status under DESA.

DSIP is constituted as a **compulsory programme** within the DESA portfolio for all jurisdictions implementing DESA frameworks. Cybersecurity and data integrity are foundational to lawful digitalisation; therefore, DSIP is not elective. Its compulsory status applies to the establishment of national CERT functions, Zero Trust architectures, SOC capabilities, and breach notification protocols. Elective modules may include advanced threat intelligence sharing and AI-driven anomaly detection, provided baseline compliance is achieved.

2.2. Purpose.

The programme’s purpose is to institutionalise sovereign cybersecurity governance and data integrity controls across all DESA assets, ensuring resilience against cyber threats, lawful processing of personal and institutional data, and demonstrable compliance with international and regional standards. DSIP operationalises these objectives through layered security architectures, privacy-by-design principles, and continuous staff capacity building, thereby safeguarding public trust and enabling uninterrupted service delivery.

2.3. Alignment with Continental and Regional Frameworks.
DSIP is aligned with the following frameworks and strategies:

- **African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)** — establishing normative obligations for data protection, cybersecurity governance, and incident response across member states.

- **Agenda 2063** — reinforcing aspirations for inclusive prosperity and governance credibility through secure digital infrastructure.

- **Agenda for Social Equity 2074** — embedding ethical principles and social safeguards in digital governance.

- **AfDB High 5 priorities** — particularly *Integrate Africa* and *Improve the Quality of Life for the People of Africa*, by enabling trusted digital ecosystems and reducing systemic risk.

- **Regional Strategies (COMESA, SADC, EAC)** — harmonising cybersecurity standards, interoperability protocols, and CERT coordination mechanisms to support cross-border resilience and lawful data exchange.

2.4. Legal Bases and Instrument Hierarchy.
DSIP derives authority from its Programme Charter, Host Country Agreement, and DESA Operating Circulars on cybersecurity and data governance. These instruments incorporate by reference the Malabo Convention, ISO/IEC 27001 for information security management, and NIST Cybersecurity Framework principles adapted for sovereign contexts. Compliance obligations include breach notification standards, algorithmic transparency for security analytics, and grievance redress mechanisms for affected stakeholders.

2.5. Relationship with GSIA and Compliance Governance
The DESA Security & Integrity Program (DSIP) operates under the overarching compliance and governance framework administered by the Global Social Impact Alliance (GSIA). GSIA functions as the external monitoring and validation entity for all DESA programmes, including DSIP, ensuring that cybersecurity and data integrity obligations are harmonised with continental and regional governance standards.

Under this relationship, GSIA assumes the following roles:

- **Policy Harmonisation and Oversight**: GSIA validates DSIP Operating Circulars against global and regional compliance benchmarks, including the Malabo Convention, ISO/IEC 27001, and emerging African Union cybersecurity directives.

- **Independent Audit and Verification**: GSIA conducts periodic audits of DSIP implementation, covering Zero Trust architecture deployment, CERT operational readiness, SOC performance, and breach notification compliance. Audit findings are disclosed through DESA's unified Monitoring, Evaluation, and Learning (MEL) dashboard.

- **Cross-Border Coordination**: GSIA facilitates interoperability of cybersecurity protocols across Regional Economic Communities (RECs), ensuring lawful data exchange and coordinated incident response for cross-border threats.
- **Ethical and Social Safeguards**: GSIA enforces alignment with Agenda for Social Equity 2074 principles, embedding transparency, accountability, and inclusion safeguards in DSIP's governance model.

This governance linkage ensures that DSIP is not an isolated technical programme but a legally integrated component of DESA's institutional architecture, subject to independent compliance verification and harmonisation with continental cybersecurity norms.

Chapter 3. Strategic Objectives

3.1. Policy Orientation and Legal Basis

The DESA Security & Integrity Program (DSIP) is established as a compulsory instrument within the DESA portfolio to safeguard the confidentiality, integrity, and availability of all DESA assets. Its strategic orientation is grounded in the principles of Malabo Convention on Cyber Security and Personal Data Protection, complemented by ISO/IEC 27001 for information security management and NIST Cybersecurity Framework principles adapted for sovereign contexts. DSIP operationalises these standards through national legal instruments, institutional governance structures, and technical architectures that enforce Zero Trust principles, privacy by design, and continuous monitoring.

The programme's legal mandate extends beyond technical compliance; it institutionalises cybersecurity as a governance function, embedding accountability and resilience into national digital ecosystems. By doing so, DSIP ensures that digitalisation under DESA is not only innovative but lawful, ethical, and socially inclusive.

3.2. Strategic Objectives

DSIP pursues five interdependent objectives, each designed to advance governance, education, markets, and social equity:

Objective I — Institutionalisation of Cybersecurity Governance
DSIP mandates the creation of sovereign cybersecurity governance structures, including a national Computer Emergency Response Team (CERT) and a Security Operations Center (SOC). These entities provide continuous threat monitoring, incident response, and compliance enforcement, reducing systemic risk and strengthening public trust in digital services.

Objective II — Deployment of Zero Trust Architectures and Privacy by Design
The programme enforces Zero Trust principles across all DESA assets, ensuring that no user or device is inherently trusted and that access is continuously verified. Privacy by design is embedded into system development lifecycles, guaranteeing lawful processing of personal data and compliance with international data protection norms.

Objective III — Capacity Building and Cyber Hygiene Certification
DSIP institutionalises cybersecurity education through mandatory training tracks and certification pathways for civil servants, technical staff, and private sector actors. This objective advances workforce competence, mitigates human-factor vulnerabilities, and creates a skilled talent pool aligned with continental priorities under Agenda 2063 and Agenda 2074.

Objective IV — Threat Intelligence and Incident Response Readiness
The programme establishes national and regional threat intelligence sharing protocols, enabling proactive detection and rapid containment of cyber threats. Incident response frameworks are codified in Operating Circulars, with mandatory breach notification standards and escalation pathways to ensure transparency and accountability.

Objective V — Compliance Assurance and Ethical Safeguards
DSIP embeds compliance verification into its governance architecture through independent audits, algorithmic transparency for security analytics, and grievance redress mechanisms for affected stakeholders. These safeguards uphold ethical principles and reinforce institutional legitimacy.

3.3. Contribution to Governance, Education, Markets, and Social Equity

- **Governance**: DSIP strengthens institutional resilience by embedding cybersecurity into national governance frameworks, reducing vulnerability to systemic disruptions and enhancing public trust.
- **Education**: Through structured training and certification, DSIP elevates national capacity in cybersecurity, creating a skilled workforce capable of sustaining secure digital ecosystems.
- **Markets**: By enforcing security and integrity standards, DSIP fosters investor confidence and stimulates private sector participation in secure digital infrastructure projects.
- **Social Equity**: Privacy by design and grievance redress mechanisms protect individual rights, ensuring that digitalisation does not compromise personal freedoms or exacerbate exclusion.

Table 3-A — Strategic Objectives and Governance Linkages

Objective	Governance Contribution	Education Impact	Market Activation	Social Equity
Cybersecurity Governance	Institutional resilience; lawful frameworks	Policy literacy for civil servants	Creates demand for secure tech solutions	Protects citizens from systemic risk
Zero Trust & Privacy by Design	Reduces insider threats; enforces lawful processing	Integrates privacy principles into curricula	Stimulates compliance-driven innovation	Guarantees personal data protection
Capacity Building	Embeds cyber hygiene in civil service	Creates certified workforce	Expands cybersecurity job market	Promotes inclusive participation
Threat Intelligence & Response	Accelerates containment; reduces downtime	Practical labs for incident response	Enables managed security services	Ensures transparency in breach handling
Compliance & Ethics	Independent audits; algorithmic transparency	Ethics modules in training tracks	Builds trust for PPP frameworks	

3.4. Institutional Objectives

The DESA Security & Integrity Program (DSIP) translates its policy-level goals into binding operational targets across national and regional cybersecurity ecosystems. These objectives are structured to ensure lawful, resilient, and scalable security architectures that protect DESA assets and national digital infrastructure.

Objective A — Establishment of Sovereign Cybersecurity Governance Structures

Every participating state shall constitute a **National Cybersecurity Authority** under its DESA Programme Office, responsible for policy enactment, compliance oversight, and coordination with regional bodies. This authority will supervise the national CERT and SOC, ensuring continuous threat monitoring and lawful incident response.

Objective B — Operationalisation of Zero Trust and Privacy by Design

DSIP mandates the deployment of Zero Trust architectures across all DESA systems, enforcing continuous identity verification and least-privilege access. Privacy by design principles shall be embedded in all system development lifecycles, ensuring compliance with Malabo Convention obligations and national data protection laws.

Objective C — Institutional Capacity Building and Certification

Cyber hygiene and security literacy shall be institutionalised through mandatory training tracks for civil servants, technical staff, and private sector actors. Certification pathways will be codified under DESA Operating Circulars and accredited by the DESA Central Unit, creating a skilled workforce capable of sustaining secure digital ecosystems.

Objective D — Threat Intelligence and Incident Response Frameworks

National SOCs shall implement real-time threat detection and automated alerting systems, integrated with regional threat intelligence platforms. Incident response protocols—including breach notification standards and escalation pathways—shall be codified in Operating Circulars and enforced through compliance audits.

Objective E — Compliance and Ethical Governance

Independent audits, algorithmic transparency for security analytics, and grievance redress mechanisms shall be institutionalised to uphold ethical principles and reinforce public trust. Compliance verification will be conducted under GSIA oversight and disclosed through DESA's unified Monitoring, Evaluation, and Learning (MEL) dashboard.

3.5. Implementation Logic and Operational Targets

DSIP adopts a **three-tier implementation model**—Infrastructure, Application, and Capacity—executed through phased sequencing to ensure legal sufficiency and operational resilience.

Table 3-B — Three-Tier Model and Binding Targets

Tier	Definition	Binding Targets	Verification
Infrastructure	Hosting, network security, identity and access management, observability	National SOC operational; Zero Trust enforced; ISO/IEC 27001 certification maintained; encrypted data flows; audit trails active	Independent security audits; penetration tests; compliance certificates

Tier	Definition	Binding Targets	Verification
Application	Threat detection, incident response, breach notification, privacy controls	CERT fully functional; automated alerting integrated; breach notification within statutory timelines; privacy by design enforced	Functional acceptance tests; breach response logs; privacy compliance audits
Capacity	Workforce training, certification, adoption support	Cyber hygiene certification for all civil servants; advanced security training for SOC staff; private sector adoption programmes	Certification registry checks; adoption metrics; quarterly compliance reports

3.6. Sequencing and Phasing

Implementation shall proceed through three operational phases, preceded by preparatory initiation:

- **Phase 0 — Initiation (Months 0–3)**
  Legal enactment of cybersecurity instruments; establishment of Programme Office and governance committees; baseline risk assessments; procurement pre-qualification for SOC tooling.

- **Phase 1 — Scale-Up (Months 3–12)**
  Deployment of SOC and CERT capabilities; implementation of Zero Trust architecture; delivery of foundational cyber hygiene training; activation of breach notification protocols.

- **Phase 2 — Consolidation (Months 12–24)**
  Integration of advanced threat intelligence platforms; institutionalisation of privacy by design in all DESA systems; accreditation of training institutions; publication of annual compliance reports.

3.7. Minimum Performance Thresholds

Binding thresholds include:

- Incident response time reduced to ≤ 4 hours for critical events by Phase II
- Breach notification issued within 72 hours of detection
- 100% of DESA systems operating under Zero Trust principles by Phase II
- Cyber hygiene certification coverage of ≥ 90% of civil servants by Phase III

3.8. Governance Architecture and Legal Sufficiency

The governance structure of DSIP is designed to ensure institutional legitimacy, operational accountability, and compliance with ethical and regulatory standards. It establishes a multi-tiered system integrating oversight, implementation, and certification functions within the broader DESA governance framework, while maintaining alignment with national laws, REC protocols, and international best practices. Importantly, DSIP governance incorporates DAIP principles wherever AI-driven security analytics are deployed, ensuring algorithmic transparency, bias audits, and ethical safeguards.

3.9. Multi-Tiered Governance Structure

DSIP governance shall be constituted under the following tiers:

a) **Central Oversight**

The DESA Central Unit serves as the supreme governing authority for DSIP, responsible for policy formulation, standard-setting, and accreditation. It operates under the Institutional Governance Manual and coordinates strategic partnerships with continental bodies (AUC, AfDB) and RECs (COMESA, SADC, EAC). It also enforces DAIP-aligned ethical AI standards for security operations.

b) **National Programme Office**

Each Host Country shall establish a DSIP Programme Office under its national DESA steering committee. This office oversees SOC and CERT operations, Zero Trust deployment, and compliance with privacy-by-design principles. It reports quarterly to the DESA Central Unit and ensures integration of DAIP's AI ethics modules into security analytics workflows.

c) **Advisory Board**

A DSIP Advisory Board provides strategic guidance and technical validation. Membership includes AfDB, GSIA, REC representatives, academia, and private sector partners. The Board convenes biannually to review progress, validate compliance with Malabo principles, and adjudicate ethical AI governance under DAIP.

3.10. Programme Office Structure

The Programme Office shall maintain the following directorates:

- **Legal and Compliance Directorate**: Drafts and enforces Operating Circulars, DPIAs, breach notification standards, and algorithmic accountability statements.

- **Technical Security Directorate**: Oversees SOC and CERT operations, Zero Trust architecture deployment, and AI-driven threat analytics under DAIP safeguards.

- **Capacity and Certification Directorate**: Manages cyber hygiene training, DAIP-integrated AI ethics modules, and certification pathways for public and private actors.

- **Monitoring and Evaluation Directorate**: Maintains KPI dashboards, conducts audits, and publishes compliance reports aligned with MEL and DAIP frameworks.

- **Finance and Fiduciary Directorate**: Administers budget envelopes, procurement protocols, and cost-control measures under DESA fiduciary standards.

3.11. Steering Committees and Reporting Lines

The national steering committee includes senior representatives from health, ICT, finance/planning, and justice ministries, alongside civil society and private sector observers. Reporting lines are structured as:

- Programme Office → National Steering Committee → DESA Central Unit

- Quarterly compliance reports → Biannual Advisory Board reviews → Annual public performance disclosure via MEL dashboard.

3.12. Compliance Mechanisms and Enforcement

Compliance is enforced through independent audits covering cybersecurity controls, AI ethics (DAIP), data governance, and accessibility. Mandatory instruments include:

- **Bias and Algorithmic Transparency Audits** for AI-driven threat detection systems.

- **Grievance Redress Mechanisms** for stakeholders affected by security incidents or algorithmic decisions.
- **Corrective Action Protocols** with time-bound remediation; persistent non-compliance triggers suspension of privileges and funding reallocation.

Table 3-C — Governance Tiers and Core Responsibilities

Tier	**Core Responsibilities**	**DAIP Integration**
Central Oversight	Policy formulation; accreditation; REC harmonisation	Enforces ethical AI standards for security analytics
National Programme Office	SOC/CERT operations; Zero Trust deployment; compliance	Integrates DAIP ethics modules into threat analytics
Advisory Board	Strategic guidance; compliance validation; dispute resolution	Reviews algorithmic transparency and bias audit reports

3.13. Legal Foundations and Normative Instruments

Compliance under DSIP is grounded in a hierarchy of binding instruments:

- **Programme Charter and Host Country Agreement**, which confer sovereign authority and define obligations for cybersecurity governance and data integrity.
- **Operating Circulars**, adopted by the national steering committee and filed with the DESA Central Unit, covering Zero Trust enforcement, breach notification standards, and algorithmic accountability for AI-driven security analytics.
- **International and Regional Standards**, incorporated by reference, including the Malabo Convention, ISO/IEC 27001, and DAIP ethical AI principles for transparency and bias mitigation.

3.14. Data Protection and Privacy Compliance

All personal and institutional data processed under DSIP must comply with national data protection laws and regional interoperability protocols. Mandatory safeguards include:

- **Data Protection Impact Assessments (DPIAs)** for SOC, CERT, and threat intelligence systems.
- **Encryption** of sensitive data at rest and in transit; role-based access controls; and secure hosting within approved jurisdictions.
- **Audit Trails and Provenance Logging** for all security events and algorithmic decisions. Cross-border threat intelligence exchange shall be subject to harmonised standards validated by the Advisory Board and REC instruments.

3.15. Algorithmic Transparency and Ethical AI

Where DSIP employs AI-driven security analytics (e.g., anomaly detection, predictive threat modelling), compliance with DAIP principles is mandatory:

- **Bias Audits** prior to deployment;
- **Explainability Reports** detailing model logic and decision pathways;
- **Human-in-the-Loop Protocols** for critical security decisions;

- **Grievance Redress Mechanisms** for stakeholders affected by algorithmic outputs. Independent audits and public disclosure of algorithmic accountability statements reinforce ethical governance.

3.16. Accessibility and Inclusion Safeguards

DSIP ensures that security and privacy controls do not create barriers for persons with disabilities or marginalised groups. Accessibility obligations include:

- **Accessible Security Interfaces** for administrative portals;
- **Inclusive Training Materials** for cyber hygiene certification;
- **Compliance with WCAG and DESA accessibility benchmarks** in all user-facing security systems.

3.17. Grievance Redress and Audit Obligations

A multi-channel grievance mechanism shall be maintained for individuals and institutions affected by security incidents or compliance breaches. Independent audits will cover:

- Cybersecurity controls and Zero Trust enforcement;
- AI ethics and algorithmic transparency;
- Data governance and privacy compliance;
- Fiduciary stewardship of security investments.

  Audit findings and corrective actions shall be disclosed through DESA's unified Monitoring, Evaluation, and Learning (MEL) dashboard.

3.18. Risk Management and Contingency Protocols

Risk categories—ethical, algorithmic, privacy, operational, and financial—are addressed through preventive and corrective measures. Mandatory safeguards include documented risk registers, time-bound remediation plans, and escalation protocols for persistent non-compliance. Significant risk events and remediation outcomes shall be disclosed publicly to maintain stakeholder confidence.

Table 3-D — Compliance Domains and Verification Mechanisms

Compliance Domain	**Mandatory Instrument**	**Verification Method**
Cybersecurity Governance	Operating Circulars; SOC/CERT charters	Independent audits; MEL dashboard disclosure
Data Protection	DPIAs; Encryption standards	Privacy compliance audits; breach logs
Algorithmic Ethics	Bias audits; Explainability reports	Pre-deployment certification; public accountability statements
Accessibility	WCAG compliance; DESA benchmarks	Disability cohort testing; remediation logs
Security Certification	ISO/IEC 27001; Incident reporting	Annual surveillance audits; penetration tests

Chapter 4 — Implementation Framework (Infrastructure, Application, Capacity, and Sequencing)

4.1 Scope and Purpose

This Chapter establishes the operational architecture of the DESA Security & Integrity Program (DSIP), setting out the three-tier model for delivery, the sequencing and phasing logic, fiduciary and financing instruments, compliance and ethics safeguards aligned with DAIP ethical AI and accessibility principles, regional harmonisation with COMESA–SADC–EAC standards, programme benefits and economic rationale, Measurement–Reporting–Verification (MRV), stakeholder engagement and capacity building, the participation and partnership framework, and the closing statement of Chapter 4. Where regulatory references are invoked—for data protection, accessibility, accountability and PPP standards—this Chapter cites authoritative instruments to ensure traceability and enforceability.

4.2 Three-Tier Model: Infrastructure, Application, Capacity

4.2.1 Tier I — Infrastructure (Trust & Resilience Layer)

The Infrastructure Tier comprises secure cloud/on-premise facilities, network and fiber backbones, sovereign data facilities, cryptographic key management, identity and access management (IAM), audit logging, and business continuity/disaster recovery (BC/DR) estates. It is designed to meet continental data governance principles and accessibility standards, ensuring lawful processing, integrity, and resilience. This Tier must be aligned with the African Union Data Policy Framework (AUDPF), which mandates harmonised data governance and trusted environments to unlock value while preventing harm, and should adopt WCAG 2.2 for all DSIP public-facing services to ensure inclusive accessibility.

4.2.2 Tier II — Application (Assurance & Controls Layer)

The Application Tier encompasses DESA security services and tools: data protection impact assessments (DPIA), algorithmic risk assessments, threat detection and incident response, zero-trust architectures, secure DevSecOps pipelines, and transparency modules for AI systems. In accordance with the OECD AI Recommendation (2019; updates 2024), DSIP enforces transparency, explainability, robustness and accountability across the AI lifecycle, including model documentation, bias testing, and redress pathways for affected parties.

4.2.3 Tier III — Capacity (People & Institutions Layer)

The Capacity Tier covers governance bodies, supervisory authorities and DESA units responsible for compliance, audit, training and certification. It integrates ministries, regulators, academia and private sector actors through designated training tracks and professional certifications. This Tier operationalises lawful bases, cross-border data flow safeguards and PPP capacities per AfDB's PPP Strategic Framework (2021–2031).

4.3 Sequencing: Initiation, Scale-Up, Consolidation

4.3.1 Phase I — Initiation (Months 0–12)

Activities: readiness diagnostics; legal and policy mapping; baseline cybersecurity controls; accessibility remediation plan; pilot grievance mechanisms and public dashboards; initial blended-finance structuring. Regulatory anchors include GDPR for data subject rights and DPIA, AUDPF for continental harmonisation, and WCAG 2.2 AA conformance for all DSIP portals.

4.3.2 Phase II — Scale-Up (Months 12–36)

Activities: fiber corridor activation for priority sectors; expansion of AI assurance tooling; roll-out of interoperable data platforms; PPP procurement; tariff safeguard regimes and affordability mechanisms; regional replication pilots with COMESA–SADC–EAC compatibility.

4.3.3 Phase III — Consolidation (Months 36–60+)

Activities: independent audits; institutionalising supervisory functions; consolidated MRV and open dashboards; formalisation of regional shared services; refinancing via performance-linked instruments; codification of grievance redress within AfDB IRM pathways.

4.4 Fiduciary Architecture and Financing Instruments

4.4.1 Structure

The DSIP adopts a blended finance architecture combining concessional windows, PPP project finance, and private capital mobilisation. It integrates with the DESA Technology & Innovation Fund (DTIF) as a ring-fenced vehicle for AI assurance, accessibility upgrades, cybersecurity and fiber-capacity co-financing. Blended-finance design follows DFI Working Group principles: clear development rationale, additionality, proportional concessionality, and avoidance of competitive distortion. [afdb.org], [ifc.org]

4.4.2 Instruments

Eligible instruments include: viability-gap grants; performance-based grants for accessibility and AI transparency; subordinated debt; guarantee facilities; revenue-backed notes; PPP availability payment structures per AfDB PPP Strategic Framework. [afdb.org]

4.4.3 Tariff Safeguards and Affordability Targets

DSIP requires affordability covenants in PPP contracts, including lifeline tariffs for essential digital public services, social tariffs for low-income households, and ex-ante tariff review mechanisms linked to MRV data. These safeguards support social equity and competitive markets under COMESA regional integration aims and AfDB's Ten-Year Strategy cross-cutting equity priorities. [leap.unep.org], [afdb-org.kr]

Table 4-A: Financing Instruments and Use Cases

Instrument	Use Case	Safeguard
Viability-gap grant	Fiber security overlays; accessibility retrofits	OECD-DAC blended finance guidance (development rationale) [oecd.org]
Subordinated debt	AI assurance platform deployment	Concessionality proportional to risk and impact (DFI WG) [ifc.org]
Partial risk guarantee	PPP cyber SOC build-operate	AfDB PPP Strategic Framework risk sharing principles [afdb.org]
Performance-based grant	Public dashboards; algorithmic transparency	OECD AI transparency/explainability principles [wecglobal.org]

4.5 Compliance and Ethics

4.5.1 Legal Bases and Data Protection

DSIP enforces lawful processing, data subject rights, DPIA, and safeguards against automated decision-making harm consistent with GDPR. For African jurisdictions, DSIP applies AUDPF, SADC Data Protection Model Law guidance, and emerging EAC data governance frameworks, ensuring regional harmonisation and adequacy of cross-border flows.

4.5.2 Algorithmic Transparency and Inclusion

All DSIP AI services must meet OECD AI principles of transparency, human-centred values, robustness and accountability; inclusive design and equitable access are mandatory, with WCAG 2.2 AA as the baseline for public interfaces.

4.5.3 Grievance Redress and Audit

DSIP establishes a dual grievance pathway: an internal DESA complaint mechanism with time-bound remedies, and escalation to AfDB's Independent Recourse Mechanism (IRM) for AfDB-financed components. Annual independent audits assess compliance with data protection, AI transparency, and accessibility covenants.

4.6 Regional Replication and Integration

4.6.1 COMESA Alignment

DSIP interoperates with COMESA's Inclusive Digitalisation (IDEA) Programme knowledge and capacity platforms and the COMESA Medium-Term Strategic Plan pillars of physical connectivity and market integration. Shared infrastructure and knowledge repositories will be hosted at DESA regional nodes, open to Member States under Operating Circulars.

4.6.2 SADC and EAC Harmonisation

DSIP legal safeguards will reflect the SADC Model Law on Data Protection and EAC model ICT policy norms, while tracking the EAC Data Governance Policy Framework validation and subsequent adoption processes. This ensures consistent privacy, cybersecurity and interoperability across regions.

4.7 Programme Benefits and Economic Rationale

4.7.1 Expected Outcomes and Quantification

DSIP is expected to deliver material benefits:

- Employment: security operations centres, compliance units, accessibility teams and AI assurance labs generate high-skill jobs with PPP mobilisation under AfDB's PPP framework.
- Cost Savings: standardised governance and shared services reduce duplicative spend and compliance failure risks, consistent with COMESA's drive for connectivity and integrated markets.
- Service Efficiency: lawful data flows, transparent AI, and WCAG-compliant services increase uptake and productivity; AUDPF emphasises trusted digital environments for inclusive economic gains.

4.7.2 Competitiveness and Social Equity

By lowering transaction costs through harmonised standards and PPP capacity, DSIP enhances national competitiveness; tariff safeguards and accessibility baselines reinforce social equity in line with AfDB's Ten-Year Strategy priorities.

4.8 Measurement, Reporting, and Verification (MRV)

4.8.1 KPI Families

DSIP adopts five KPI families:

1. **Security & Integrity**: incident mean-time-to-detect/respond; audit log completeness; zero-trust maturity.
2. **Data Protection & Ethics**: DPIA coverage; lawful-basis mapping; algorithmic transparency scores under OECD-aligned rubrics.
3. **Accessibility**: WCAG 2.2 AA conformance rates; usability scores for assistive technologies.

4. **Affordability & Inclusion**: lifeline tariff adoption; low-income household coverage; multilingual access metrics aligned with COMESA/EAC norms.
5. **Finance & PPP**: blended-finance leverage ratio; private capital mobilisation; PPP availability payment performance per AfDB framework.

4.8.2 Reporting Cadence and Public Dashboards

Quarterly MRV reporting to the DESA central unit; semi-annual publication of open dashboards; annual independent audit referencing AfDB IRM accountability guidance for grievance statistics and remediation outcomes.

4.9 Stakeholder Engagement and Capacity Building

4.9.1 Engagement Model

Structured engagement with ministries (ICT, Justice, Finance), regulators, academia, private sector and civil society through Working Parties and Operating Circulars. COMESA's regional knowledge and capacity platform is utilised for shared curricula and toolkits.

4.9.2 Training Tracks and Certification Pathways

Tracks include: Data Protection Officer; AI Assurance Lead; Accessibility Engineer (WCAG 2.2); PPP Contracting Authority Specialist. Certifications reference GDPR, AUDPF, OECD AI and WCAG guidance, and PPP modules under AfDB's framework.

4.10 Participation and Partnership Framework

4.10.1 Instruments

Participation is formalised via Memoranda of Understanding (MoUs), Operating Circulars and Partner Entry Conditions. Priority partners include DFIs (AfDB and others under DFI WG), investors, telecoms/fiber consortia, accessibility and AI assurance providers.

4.10.2 Calls to Action (CTAs)

- **Investors/DFIs**: commit concessional tranches and guarantees in line with DFI blended-finance principles and AfDB PPP Strategic Framework.
- **Technology Partners**: co-develop transparency modules and accessibility upgrades, certifying conformance to OECD AI and WCAG 2.2.
- **Regulators/Member States**: adopt Operating Circulars for harmonised grievance redress, data protection and PPP procurement. Align with AUDPF and regional model laws.

4.11 Closing Statement

This Implementation Framework operationalises DSIP as a sovereign, ethical and scalable solution within DESA's long-term vision. Through a layered architecture, disciplined phasing, lawful AI and accessibility safeguards, blended financing and PPP mobilisation, and regionally harmonised standards and MRV, DSIP delivers a compliant, inclusive, and economically rational security and integrity programme for national and regional digital ecosystems.

Chapter 5 — Governance, Risk, and Safeguards

5.1 Purpose and Scope

This Chapter codifies the governance system, risk taxonomy, safeguards, and assurance mechanisms through which DSIP maintains legality, ethical integrity, cybersecurity resilience, data protection, algorithmic transparency, accessibility, and fiduciary probity. It complements the Legal Mandate and Compliance provisions of Chapters 1–3 and the Implementation Framework of Chapter 4 by operationalising oversight bodies, control processes, risk treatment pathways, and redress mechanisms consistent with continental and international instruments. The framework is explicitly anchored in the African Union Data Policy Framework (AUDPF), the EU General Data Protection Regulation (GDPR), the OECD Recommendation on Artificial Intelligence (AI), WCAG 2.2 accessibility standards, and regional harmonisation under COMESA, SADC, and EAC.

5.2 Governance Architecture

5.2.1 Oversight Bodies and Lines of Authority

DSIP governance is exercised through a multi-layer architecture:

a) **DESA Central Security & Integrity Board (CSIB)**, mandated to approve security policies, oversee fiduciary and compliance risk, and authorise corrective actions; it aligns programme controls with AUDPF's trusted data environment and cross-border governance guidance.

b) **Independent Audit & Ethics Committee (IAEC)**, charged with annual external audits of data protection, AI transparency, accessibility conformance (WCAG 2.2), and PPP fiduciary integrity, reporting to CSIB and to relevant DFIs when DSIP components are co-financed under PPP structures per AfDB's PPP Strategic Framework.

c) **Supervisory Authorities Interface Unit (SAIU)**, a specialist liaison cell that harmonises DSIP controls with national regulators and regional standards (COMESA, SADC, EAC) to ensure adequacy of data protection, cybersecurity and ICT policy alignment.

d) **Grievance and Remedy Office (GRO)**, managing internal grievance processes and escalation matrices to AfDB's Independent Recourse Mechanism (IRM) for AfDB-financed components, thereby embedding independent recourse in the governance model.

5.2.2 Delegation Instruments

Governance obligations are formalised through Operating Circulars, Directives, and MoUs with partners and regulators, ensuring enforceable controls and auditability consistent with GDPR's accountability principle and AUDPF's harmonisation intent.

5.3 Risk Taxonomy and Control Framework

5.3.1 Risk Families

DSIP adopts a standardised taxonomy:

1. **Cybersecurity & Operational Integrity Risks**: network intrusions, ransomware, supply-chain compromise, incident response latency.
2. **Data Protection & Privacy Risks**: unlawful processing, inadequate lawful bases, weak DPIA practice, cross-border transfer non-compliance.
3. **Algorithmic & AI Risks**: opacity, bias, robustness failures, unsafe deployment and lack of accountability.
4. **Accessibility & Inclusion Risks**: non-conformance with WCAG 2.2, exclusion of users with disabilities, language and affordability barriers.
5. **Fiduciary & PPP Risks**: procurement irregularities, tariff inequity, weak availability-payment governance, inadequate blended-finance additionality.

5.3.2 Control Objectives

Controls are aligned with: GDPR controller/processor duties and DPIA requirements; AUDPF's safe and trustworthy data environment mandate; OECD AI transparency/robustness/accountability; WCAG 2.2 AA conformance for public-facing services; AfDB PPP governance and blended-finance discipline for private capital mobilisation.

5.4 Safeguards by Domain

5.4.1 Data Protection and Privacy

DSIP enforces lawful bases, data subject rights, DPIA, records of processing, breach notification and cross-border transfer adequacy consistent with GDPR Chapter II–V. For African contexts, DSIP references AUDPF and SADC Model Law on Data Protection to support legislative harmonisation and supervisory capacity, and tracks EAC's evolving Data Governance Policy Framework to align partner-state practices.

5.4.2 Algorithmic Transparency and AI Assurance

All DSIP AI systems must: disclose AI interaction, document datasets/model lineage, conduct bias and performance testing, implement human-in-the-loop or equivalent oversight for high-risk use, and publish explainability artefacts proportionate to risk, consistent with the OECD AI Recommendation and its transparency/robustness/accountability principles.

5.4.3 Accessibility and Inclusion

DSIP mandates WCAG 2.2 AA conformance for web and app services, with periodic audits and remediation roadmaps to address perceivable, operable, understandable and robust design principles, ensuring inclusive usage and legal defensibility in accessibility procurement and PPP service design.

5.4.4 Cybersecurity and Operational Integrity

Zero-trust segmentation, privileged access management, multi-factor authentication, immutable logging, threat intelligence integration, and tested BC/DR plans are prescribed as minimums. Regional interoperability is pursued via COMESA connectivity strategies and EAC/SADC policy models to ensure consistent cyber hygiene across borders.

5.4.5 Fiduciary and PPP Safeguards

Procurement is governed by transparent PPP rules, competitive tendering, availability-payment performance metrics, tariff social safeguards, and blended-finance tests for additionality and proportionality per DFI Working Group guidance and AfDB's PPP Strategic Framework.

5.5 Grievance Redress, Remedies, and Accountability

5.5.1 Internal Mechanism

The GRO maintains a multi-channel complaint intake, triage, investigation and remedy issuance with time-bound service levels and public reporting. Outcomes include correction, explanation, compensation (where applicable), and systemic improvement directives.

5.5.2 External Escalation

Where DSIP components are AfDB-financed, complainants may escalate to the AfDB IRM, which provides independent recourse and mediation or compliance review, binding DSIP to continental accountability standards.

5.5.3 Audit and Public Disclosure

Annual independent audits cover data protection, AI assurance, accessibility conformance and PPP fiduciary integrity; summary reports are published via open dashboards consistent with Chapter 4 MRV commitments.

5.6 Cross-Border Harmonisation and Regional Compliance

5.6.1 COMESA

DSIP aligns with COMESA's Medium-Term Strategic Plan pillars and leverages the IDEA Programme's regional planning and knowledge platforms to standardise cyber, data and accessibility practices, reducing compliance latency across Member States.

5.6.2 SADC and EAC

DSIP applies SADC's Model Law guidance to national legislative gaps and supports EAC's Data Governance Policy Framework adoption to achieve interoperable, trusted cross-border flows and ICT services.

5.7 Risk Treatment Pathways

5.7.1 Identification and Assessment

Risks are catalogued in the DSIP Risk Register, scored by likelihood–impact, mapped to control owners, and reviewed quarterly by CSIB and IAEC.

5.7.2 Treatment and Escalation

Treatment options—avoid, mitigate, transfer, accept—are chosen based on regulatory obligations (e.g., GDPR DPIA outcomes), ethical implications (OECD AI), and accessibility imperatives (WCAG 2.2). Material risks trigger Operating Circulars and corrective actions, with possible AfDB IRM notification where relevant.

5.8 Table 5-A: Risk–Control–Assurance Mapping

Risk Family	**Key Controls**	**Assurance & Reference**
Data Protection	Lawful bases; DPIA; breach notification; transfer safeguards	GDPR Chapters II–V; AUDPF implementation notes
Algorithmic/AI	Documentation; explainability; bias testing; human oversight	OECD AI transparency/robustness/accountability
Accessibility	WCAG 2.2 AA audits; remediation; user testing	WCAG 2.2 Recommendation; quarterly MRV
Cybersecurity	Zero-trust; PAM; MFA; immutable logs; BC/DR	Regional policy alignment (COMESA/EAC/SADC)
PPP/Fiduciary	Competitive tendering; availability metrics; tariff safeguards	AfDB PPP Strategic Framework; DFI WG principles

5.9 Continuous Improvement and Knowledge Management

DSIP institutes quarterly reviews of controls, semi-annual stakeholder exercises (ministries, regulators, academia, civil society), and annual policy refreshes to incorporate updates to regional frameworks and international instruments (e.g., OECD AI updates, WCAG revisions), thereby sustaining compliance, ethics and resilience at scale.

5.10 Closing Statement

The governance, risk and safeguards architecture of DSIP provides a legally rigorous, ethically sound, and regionally interoperable system for security and integrity. By embedding accountability, accessibility, lawful data protection, transparent AI, and robust PPP fiduciary disciplines, DSIP ensures enforceable protections for users and institutions while enabling efficient, compliant and inclusive digital public infrastructures across COMESA, SADC and EAC.

Chapter 6 — Technical Standards & Assurance Profiles

6.1 Purpose and Scope

This Chapter codifies the technical standards, control baselines, and assurance profiles that govern DSIP's implementation across infrastructure, applications, and capacity domains. It establishes a multi-standard stack that is lawful, interoperable, and auditable; provides conformity assessment pathways and evidence requirements; and defines how DSIP attains presumption of conformity where relevant regulations and harmonised standards permit it. The stack aligns with established global and regional instruments, including NIST CSF 2.0, ISO/IEC 27001:2022 and companion standards, NIST SP 800-53 Rev. 5, FIPS 140-3, NIST SP 800-63-4, CSA Cloud Controls Matrix (CCM) v4, WCAG 2.2 and EN 301 549, GDPR, and the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), complemented by the OECD AI Recommendation.

6.2 Standards Stack — Core Norms and Profiles

6.2.1 Governance and ISMS

DSIP adopts NIST Cybersecurity Framework (CSF) 2.0 as the overarching governance taxonomy for cybersecurity outcomes, including the Govern function and mappings to NIST control catalogs and sector profiles, thereby structuring policy, risk strategy, roles, obligations, and supply-chain risk. For certifiable governance, ISO/IEC 27001:2022 is the mandatory Information Security Management System (ISMS) standard; the ISO/IEC 27002:2022 control guidance and attributes are referenced for implementation detail across organizational, human, physical, and technological controls.

6.2.2 Privacy and Data Protection

The GDPR provides the legal basis for processing, DPIA, data subject rights, and cross-border transfer safeguards; DSIP requires technical and organizational measures consistent with GDPR Chapters II–V. To formalise privacy governance, DSIP integrates ISO/IEC 27701 — the current 2025 edition recognised as a standalone Privacy Information Management System (PIMS) — establishing controller/processor accountability and continuous improvement for PII processing.

6.2.3 Cybersecurity Controls and Resilience

For detailed security and privacy controls, DSIP references NIST SP 800-53 Rev. 5 (including 2025 update notes and baselines) to underpin outcome-based control selection and supply-chain risk management. Business continuity and crisis readiness must conform to ISO 22301:2019 requirements for BCMS planning, operations, testing, and continual improvement.

6.2.4 Cryptography and Module Validation

All cryptographic modules used within DSIP must be FIPS 140-3 validated under CMVP, with evidence via current validation certificates and implementation guidance.

6.2.5 Digital Identity and Federation

Identity proofing, authentication, and federation must meet NIST SP 800-63-4 assurance level requirements and associated technical criteria, superseding SP 800-63-3 to reflect contemporary digital identity risks and customer-experience considerations.

6.2.6 Cloud Security and Shared Responsibility

For cloud services, DSIP applies the CSA Cloud Controls Matrix (CCM) v4 control set and associated CAIQ and STAR artefacts for assurance, mapping to ISO/NIST frameworks and clarifying shared responsibility across CSPs and customers.

6.2.7 Accessibility and ICT Procurement

Public-facing services and ICT procurement must conform to **WCAG 2.2 Level AA and the harmonised European standard EN 301 549 for ICT accessibility, ensuring functional performance across software, hardware, telecoms and support services.**

6.2.8 IoT Security Baseline

Consumer-facing DSIP deployments with connected devices shall meet ETSI EN 303 645 baseline provisions (e.g., no default passwords, coordinated vulnerability disclosure, secure update), supporting future certification schemes and aligning with EU practice.

6.2.9 AI Governance and Compliance

DSIP’s AI components observe the OECD AI Recommendation principles of transparency, explainability, robustness, security, safety and accountability across the lifecycle.
Where applicable, DSIP’s systems and documentation align with obligations under the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), including risk management, data and data governance, technical documentation, record-keeping, transparency to deployers, human oversight, accuracy/robustness/cybersecurity, and post-market monitoring.

6.3 Assurance Profiles and Conformity Assessment

DSIP defines three assurance profiles that determine minimum certification, audit, and test evidence:

a) Baseline Assurance. ISMS certification to ISO/IEC 27001; WCAG 2.2 AA conformance statement; NIST CSF 2.0 profile and governance attestation; initial privacy governance under ISO/IEC 27701; cryptographic inventory confirmed as FIPS 140-3 validated modules where cryptography is used.

b) Enhanced Assurance. Control mapping to NIST SP 800-53 baselines with independent audit; ISO 22301 certification; CCM v4 controls with CAIQ responses and publication to CSA STAR L1 or higher; NIST SP 800-63-4 evidence for identity proofing and authentication; EN 301 549 procurement clause integration.

c) Sovereign Assurance. EU AI Act conformity processes for high-risk systems (risk management, technical documentation, logging, transparency, human oversight, accuracy/robustness/cybersecurity) and post-market monitoring; expanded privacy controls under ISO/IEC 27701; IoT baseline per ETSI EN 303 645 if applicable.

Conformity assessment evidence may include accredited certifications, third-party audits, test reports, STAR submissions, CMVP certificates, and publicly accessible accessibility conformance reports.

6.4 Control Baselines and Tailoring

Table 6-A: DSIP Domains and Referenced Controls

DSIP Domain	Primary Standards & Instruments	Baseline Application

Governance & ISMS	NIST CSF 2.0;
	ISO/IEC 27001:2022;
	ISO/IEC 27002:2022
		Governance function outcomes; ISMS certification; control attributes and implementation guidance. [nist.gov], [iso.org], [iso.org]

Privacy & Data Protection	GDPR; ISO/IEC 27701:2025	Lawful basis, DPIA, rights; PIMS accountability and continual improvement. [eur-lex.europa.eu], [iso.org]
Security Controls	NIST SP 800-53 Rev. 5	Outcome-based security and privacy controls; SCRM integration. [csrc.nist.gov]
Business Continuity	ISO 22301:2019	BCMS scope, operations, testing and improvement. [iso.org]
Cryptography	FIPS 140-3; CMVP	Validated modules; implementation guidance and DTR. [csrc.nist.gov], [csrc.nist.gov], [csrc.nist.gov]
Digital Identity	NIST SP 800-63-4	Identity proofing, authentication, federation assurance levels. [csrc.nist.gov]
Cloud Security	CSA CCM v4 (with CAIQ/STAR)	Cloud control assurance; shared responsibility clarification. [cloudsecur...liance.org], [cloudsecur...liance.org]
Accessibility	WCAG 2.2; EN 301 549	AA conformance; ICT procurement and service accessibility. [w3.org], [dia.gov.cz]
IoT Baseline	ETSI EN 303 645	Consumer IoT security requirements and assessment alignment. [etsi.org]
AI Compliance	EU AI Act; OECD AI Recommendation	Risk management and obligations for high-risk AI; lifecycle ethics and transparency. [eur-lex.europa.eu], [wecglobal.org]

6.5 Evidence, Documentation, and Presumption of Conformity

DSIP documentation includes risk management records, data governance artefacts, technical documentation, logs, transparency notices to deployers, and human-oversight controls for AI systems, consistent with the EU AI Act's requirements and post-market monitoring regime. Where harmonised standards apply (e.g., EN 301 549 for ICT accessibility), DSIP utilises the harmonisation pathway to demonstrate compliance with EU directives and procuring-entity obligations, supplemented by WCAG 2.2 conformance reports.

6.6 Independent Testing and Cryptographic Validation

For modules implementing cryptography, DSIP requires FIPS 140-3 validation evidence via CMVP certificate entries and alignment to NIST implementation guidance and derived test requirements (SP 800-140). This evidence is retained in DSIP audit files and referenced in conformity statements.

6.7 Digital Identity Assurance and Federation Controls

Identity proofing, authentication mechanisms, and federation assertions must meet SP 800-63-4 technical requirements, including assurance levels, authenticator lifecycle management, and privacy considerations. DSIP records identity assurance decisions and integrates federation where appropriate to support secure service access.

6.8 Accessibility Conformance and Procurement

All DSIP public interfaces and documents adopt WCAG 2.2 AA; procurement specifications incorporate EN 301 549 clauses to ensure accessible hardware, software, telecoms, media and support, applying self-scoping and functional performance statements. Conformance testing results and remediation plans are documented within DSIP MRV.

6.9 Cloud and Supply-Chain Assurance

Cloud implementations are assessed via CCM v4 controls and CAIQ; DSIP may submit STAR Level 1 self-assessment and optionally pursue higher levels, with mappings to ISO/NIST frameworks enabling integrated audit readiness. Supply-chain transparency and accountability controls are applied per CCM domains.

6.10 IoT Device Assurance

Where DSIP deployments include consumer IoT, manufacturers and integrators must demonstrate alignment with ETSI EN 303 645 provisions, including vulnerability disclosure, secure updates, and data protection, supported by applicable assessment specifications.

6.11 Update, Review, and Change Control

DSIP reviews its standards stack annually and upon issuance of major revisions (e.g., NIST CSF 2.0 updates, ISO/IEC revisions, EU AI Act guidance, EN 301 549 updates), issuing Operating Circulars to maintain compliance and assurance integrity

Chapter 7 — Operational Security & Incident Response

7.1 Purpose and Scope

This Chapter establishes the operational doctrine, processes, and evidence requirements by which DSIP prevents, detects, triages, responds to, and recovers from cybersecurity incidents in a manner that is lawful, auditable, and interoperable across jurisdictions. It aligns incident response with the NIST Cybersecurity Framework 2.0 functions—Govern/Identify/Protect supporting Detect/Respond/Recover—and implements the current NIST SP 800-61 Revision 3 incident-response community profile. It further codifies the structured process of ISO/IEC 27035-1:2023 for incident management; integrates contingency and recovery guidance from NIST SP 800-34 Rev. 1 and NIST SP 800-184; adopts the FIRST CSIRT Services Framework for service cataloguing; and mandates threat-informed operations referencing MITRE ATT&CK® Enterprise Matrix.

7.2 Operating Model and Lines of Responsibility

7.2.1 DSIP Computer Security Incident Response Team (CSIRT)

A dedicated DSIP CSIRT is instituted with clear mandate, constituency, and service portfolio defined per the FIRST CSIRT Services Framework v2.1, including monitoring and detection, incident analysis, incident coordination, vulnerability management, and post-incident improvement. The CSIRT service catalogue is tailored to DSIP's sovereign mission and partner portfolios, acknowledging that not all services are required at all times; prioritisation follows risk and constituency mandates.

7.2.2 Governance Integration

Preparation activities—governance, asset and risk identification, protective controls—are executed under CSF 2.0. Incident response life-cycle activities (Detect, Respond, Recover) follow **SP 800-61r3**, with continuous improvement loops feeding risk governance and control enhancement.

7.3 Detection and Triage

7.3.1 Threat-Informed Detection

Detection use-cases are mapped to MITRE ATT&CK® Enterprise tactics and techniques across Windows, Linux, macOS, cloud (SaaS/IaaS), identity providers and network devices, enabling telemetry coverage analysis and prioritised alerting. Detection engineering is maintained against ATT&CK v18 updates and instrumented through SIEM/SOAR scenarios.

7.3.2 Intake, Classification, and Prioritisation

Event and incident intake mechanisms (portals, secure mail, APIs) use structured triage according to ISO/IEC 27035-1:2023 principles, ensuring timely qualification (true/false positives) and criticality-based prioritisation. Triage artefacts capture indicators, affected assets, impact assessment, and linkage to ATT&CK techniques for repeatability.

7.4 Response and Containment

7.4.1 Standard Operating Procedures (SOPs)

DSIP SOPs adopt **SP 800-61r3** recommendations for incident coordination, communication control, evidence preservation, containment and eradication decision matrices, and stakeholder notifications. SOPs are technology-agnostic to remain current across environments; implementation details are maintained in runbooks that reference community resources as advised by NIST.

7.4.2 Supply-Chain and Third-Party Incidents

Where incidents implicate suppliers or cloud services, DSIP applies ISO/IEC 27036-3:2023 guidance to gain visibility into multi-layer hardware/software/services supply chains and to integrate security practices with lifecycle processes. Contractual instruments must incorporate incident cooperation, forensic access, and notification covenants.

7.5 Recovery and Continuity

7.5.1 Technical and Organisational Recovery

Recovery planning, playbooks, testing, and metrics follow NIST SP 800-184, ensuring rapid service restoration and minimised stakeholder impact. DSIP aligns system-level contingency with NIST SP 800-34 Rev. 1, including Business Impact Analysis (BIA), preventive controls, alternate sites, and exercises.

7.5.2 Post-Incident Improvement

Lessons learned are formally captured and fed into CSF's Improvement category; corrective actions include detection use-case refinement, control coverage adjustments, and supplier performance measures under ISO/IEC 27036-3:2023.

7.6 Vulnerability Coordination and Disclosure

7.6.1 Internal Handling and External Disclosure

DSIP adopts a two-part standard model: internal handling processes per ISO/IEC 30111:2019 (verification, analysis, remediation) and external vulnerability disclosure per ISO/IEC 29147:2018, including intake channels, coordinated disclosure, and remediation communication. Public disclosures are timed to minimise exploitation risks while enabling user risk management; where IoT products are implicated, practices align with ETSI EN 303 645 top provisions (no default passwords, disclosure policy, secure updates).

7.6.2 Sector and Community Coordination

The CSIRT maintains coordination links with national/regional CERTs and follows established community guidance for coordinated disclosure, referencing programmatic precedents (e.g., JPCERT/CC and IoTSF guidelines) where applicable to DSIP's jurisdictional engagements.

7.7 Evidence, Audit, and Legal Safeguards

7.7.1 Chain of Custody and Forensics

All incident artefacts—logs, images, configurations, communications—are preserved with documented chain of custody and integrity checks, consistent with SP 800-61r3 recommendations and ISO/IEC 27035-1 process requirements.

7.7.2 Auditability and Reporting

Incident registers, corrective actions, and recovery metrics are incorporated in DSIP MRV, with quarterly reports to governance bodies and annual independent audits aligned to the control families of **NIST SP 800-53 Rev. 5** (IR, SI, CP) and ISO incident-management clauses.

7.8 Training, Exercises, and Readiness

7.8.1 Competence Development

CSIRT roles and competencies follow the FIRST framework; DSIP will support targeted training and service-maturity development through open curriculum references and exercises mapped to ATT&CK tactics.

7.8.2 Table-Top and Live Exercises

An annual programme of table-top scenarios and live simulations tests detection, decision-making, containment, communication, and recovery, with scenarios designed from recent ATT&CK-documented adversary behaviours and sector-specific supply-chain risks per ISO/IEC 27036-3.

7.9 Communications and Stakeholder Management

7.9.1 Internal Communications

Communications during incidents are governed by SP 800-61r3, ensuring need-to-know dissemination, executive briefings aligned to CSF governance, and synchronised legal/privacy notifications.

7.9.2 External Notifications

Notifications to affected parties, regulators, and partners are performed in accordance with vulnerability disclosure standards (**ISO/IEC 29147**) and contractual obligations. Public statements emphasise remediation steps, risk-mitigation guidance, and post-incident commitments.

Table 7-A: DSIP Incident Life-Cycle and Standards Cross-Reference

Life-Cycle Phase	Primary Standard(s)	Key DSIP Activities
Preparation (Govern/Identify/Protect)	NIST CSF 2.0; FIRST CSIRT; ISO/IEC 27035-1	Service catalogue; policies; playbooks; training; risk & asset baselines. [d4daccess.eu], [first.org], [iso.org]
Detect	MITRE ATT&CK; ISO/IEC 27035-1	Telemetry use-cases; ATT&CK mapping; intake and triage. [attack.mitre.org], [iso.org]
Respond	NIST SP 800-61r3	Containment; eradication; evidence; communications; coordination. [csrc.nist.gov]
Recover	NIST SP 800-184; NIST SP 800-34r1	Service restoration; contingency activation; testing; metrics. [csrc.nist.rip], [csrc.nist.gov]
Improve	NIST CSF 2.0; NIST SP 800-61r3	Lessons learned; control improvements; MRV reporting. [d4daccess.eu], [csrc.nist.gov]
Supply-Chain	ISO/IEC 27036-3	Supplier coordination; contractual safeguards; visibility. [iso.org]
Vulnerability Mgmt	ISO/IEC 30111; ISO/IEC 29147; ETSI EN 303 645	Internal handling; coordinated disclosure; IoT security updates. [iso.org], [webstore.iec.ch], [eur-lex.europa.eu]

7.10 Metrics and MRV (Measurement, Reporting, Verification)

7.10.1 KPI Families

1. **Detection Quality**: mean time to detect (MTTD), false-positive rate, ATT&CK coverage ratios. (ATT&CK mapping provides objective coverage metrics.) [attack.mitre.org]

2. **Response Efficiency**: mean time to respond/contain (MTTR/C), eradication time, communication SLAs aligned with SP 800-61r3. [csrc.nist.gov]

3. **Recovery Performance**: service-restoration time vs. Recovery Time Objectives (RTOs) from SP 800-184/800-34 planning. [csrc.nist.rip], [csrc.nist.gov]

4. **Vulnerability Lifecycle**: time-to-verify, time-to-fix, time-to-disclose per ISO/IEC 30111 and 29147. [iso.org], [webstore.iec.ch]

5. **Supply-Chain Assurance**: incident cooperation timeliness and artefact quality per ISO/IEC 27036-3. [iso.org]

7.10.2 Reporting Cadence

Quarterly CSIRT operational reports to DSIP governance; semi-annual public dashboards summarising anonymised incident statistics; annual independent audits of IR/BCMS controls against NIST SP 800-53 Rev. 5 families (IR, CP, SI).

7.11 Closing Statement

DSIP's operational security and incident response architecture provides a disciplined, standards-anchored mechanism to protect services, constituents, and partners. By integrating CSF 2.0 governance, NIST incident-response guidance, ISO incident-management processes, supply-chain security, vulnerability coordination, and threat-informed detection through ATT&CK, DSIP achieves a lawful, ethical, and resilient operating posture capable of sustaining continuity and trust at scale.

Chapter 8 — Data Governance & DPIA Execution

8.1 Purpose and Scope

This Chapter establishes DSIP's binding policy for lawful, ethical, and accountable data governance and the systematic execution of Data Protection Impact Assessments (DPIAs). It integrates the legal requirements of the GDPR including Article 35 DPIA obligations and content, and supervisory authority practices; operationalises EU AI Act Article 10 data and data-governance requirements for high-risk AI systems; and aligns enterprise privacy governance with ISO/IEC 27701:2025 and the NIST Privacy Framework to ensure risk-based accountability and continuous improvement.

8.2 Data Governance Principles and Operating Model

DSIP's governance adopts a layered model:

1. **Lawful Basis and Purpose Specification.** All processing activities must be anchored in a documented lawful basis, with explicit purpose specification and proportionality assessment under GDPR and, where AI is involved, linked to Article 10 AI Act data-governance practices covering design choices, data origin, preparation, bias examination, and remediation.

2. **Data Quality and Integrity.** Training/validation/testing datasets for high-risk AI must be relevant, sufficiently representative, and—where feasible—free of errors; they must possess appropriate statistical properties and reflect the geographical, contextual, behavioural, or functional setting of deployment.

3. **Privacy-by-Design and Accountability.** DSIP institutes an auditable Privacy Information Management System (PIMS) aligned with ISO/IEC 27701:2025 (standalone PIMS), defining roles (controller/processor), governance artefacts, KPIs, internal audits, and management review; this complements the NIST Privacy Framework's Profiles and Tiers for enterprise risk management.

4. **Bias Detection and Special Categories.** For high-risk AI systems, providers may exceptionally process special categories of personal data strictly to detect/correct bias and only with safeguards (security, minimisation, limits on reuse/transfer, deletion post-correction) in accordance with Article 10(5) AI Act and applicable EU data-protection law.

5. **International Cooperation and Interoperability.** DSIP recognises OECD Privacy Guidelines as a global benchmark (collection limitation, data quality, use limitation, security safeguards, openness, individual participation, accountability) to harmonise practices in cross-border contexts and support trusted data flows.

8.3 Data Governance Controls and Artefacts

DSIP mandates the following artefacts:

a) **Data Inventory and Records of Processing (RoP).** Comprehensive registers documenting purposes, lawful bases, categories, recipients, transfer mechanisms, retention, and safeguards; RoP entries must reference the relevant Article 10 AI Act data-governance elements for AI systems.

b) **Data Lifecycle and Quality Plans.** Plans covering collection provenance, data-preparation operations (annotation, labelling, cleaning, enrichment), statistical adequacy, error-handling, and updating cadence, consistent with AI Act Article 10(2)–(3).

c) **Bias Assessment Protocols.** Documented assumptions, bias examinations, and mitigation measures for datasets and models, including identification of gaps/shortcomings and their remediation pathways.

d) **PIMS Documentation.** Policies, risk registers, DPIA references, internal audit reports, non-conformity logs, and management-review minutes per ISO/IEC 27701:2025 governance expectations.

e) **Privacy Risk Profiles and Tiers.** Adoption of NIST Privacy Framework Profiles/Tiers to express target outcomes and maturity across DSIP units, aligned with CSF 2.0 structure for governance interoperability.

8.4 DPIA Mandate and Triggers

A DPIA is mandatory prior to processing where the activity is “likely to result in a high risk to the rights and freedoms of natural persons,” including at minimum: systematic and extensive automated decision-making with legal or similarly significant effects; large-scale processing of special-category or criminal-data; or large-scale systematic monitoring of publicly accessible areas (GDPR Article 35). Supervisory authorities also publish lists of processing subject to DPIA or exempt from DPIA (consistency mechanism applies for cross-border impacts). DSIP must consult these lists where available and apply DPIA screening to new projects and changes.
The EDPB Guidelines (WP248 rev.01) clarify DPIA scope, timing, responsibilities (controller with DPO/processors), methodology and criteria to determine “likely high risk”; DSIP’s DPIA execution follows these guidelines.

Authoritative regulators (e.g., ICO) provide operational examples—innovative technology including AI, denial of service via automated decision-making, large-scale profiling, biometrics—and best-practice DPIA templates to be used by DSIP where applicable.

8.5 DPIA Content and Evidence Requirements

Each DPIA must include, at minimum:

1. **Systematic description of processing and purposes** (including legitimate interests, where applicable).
2. **Necessity and proportionality assessment** against stated purposes and lawful basis.
3. **Risk assessment** addressing likelihood/severity of impacts to data subjects, considering automated decisions, profiling, vulnerable populations, and bias risks (AI).
4. **Safeguards and mitigation measures** (technical and organisational), including minimisation, security, access controls, retention limits, transparency, human oversight (for AI), and redress mechanisms.

5. **Consultation** with the DPO and, where appropriate, data subjects or experts; if residual high risk remains, prior consultation with the competent supervisory authority is required before processing.

Operational guidance and checklists from regulators and public bodies may be used (screening tools, templates, sector specifics) to standardise DSIP documentation.

8.6 DPIA Process and Timing

DSIP’s DPIA process is conducted **before** processing begins and at material changes:

- **Screening.** Initial check against DPIA triggers and supervisory lists; record rationale.
- **Scoping and Stakeholder Mapping.** Identify data categories, data subjects, processing operations, technologies, suppliers/processors, jurisdictions, and transfers.
- **Assessment Execution.** Perform the analysis per 8.5 with EDPB methodology; where AI is involved, embed Article 10 AI Act data-governance steps (design choices, provenance, preparation, bias).
- **Decision and Documentation.** Approve with mitigation and control plan; if residual high risk persists, initiate prior consultation with the supervisory authority (e.g., ICO timelines: typically 8–14 weeks).
- **Review and Update.** Re-assess upon changes in purpose, scope, datasets, models, or new risks; maintain version control and evidence logs.

8.7 AI-Specific Data Governance Measures

For high-risk AI systems:

a) **Data Governance Plan.** Formal plan demonstrating compliance with Article 10(2)–(4): design choices, origin and original purpose for personal data, preparation operations, assumptions, data availability/quantity/suitability, bias exam/mitigation, and gap remediation.

b) **Dataset Quality Dossier.** Evidence that datasets are relevant, representative, complete/error-managed, and statistically appropriate for intended use; contextual representativeness must be documented.

c) **Exceptional Processing of Special Categories.** Where strictly necessary for bias detection/correction and subject to safeguards, document the legal basis and limitations per Article 10(5); confirm deletion post-correction and prohibit onward transmission or reuse.

8.8 Integration with PIMS (ISO/IEC 27701:2025) and NIST Privacy Framework

DSIP’s PIMS ensures privacy governance is embedded and certifiable, independent or alongside ISMS, with management clauses (4–10), controller/processor controls, KPIs, internal audits, and management review.

The NIST Privacy Framework (v1.0; pending v1.1 finalisation) provides Profiles and Tiers to articulate risk outcomes, leadership accountability, and alignment with CSF 2.0; DSIP maps DPIA outputs to PF Core activities to ensure enterprise-wide traceability and resource optimisation.

8.9 International and Cross-Border Considerations

Where DSIP undertakes cross-border processing or transfers, governance references OECD Privacy Guidelines for interoperability and trusted flows, and applies GDPR transfer tools and risk-assessment practices within the PIMS. [oecd.org]

8.10 Metrics and MRV (Measurement, Reporting, Verification)

DSIP tracks:

- **DPIA Coverage and Timeliness:** % of in-scope projects screened and assessed pre-go-live; average time-to-DPIA completion. (Triggers per GDPR Art. 35; EDPB guidance.)
- **Dataset Quality and Bias Metrics:** representativeness indices; error rates; bias-detection outcomes and mitigation timeliness per AI Act Article 10.
- **PIMS Effectiveness:** audit findings, corrective-action closure rates, management-review decisions (ISO/IEC 27701:2025).
- **Privacy Framework Maturity:** PF Profile attainment and Tier movement (NIST PF).

8.11 Closing Statement

DSIP's data governance and DPIA regime provides a legally rigorous and operationally mature framework for privacy-by-design, dataset integrity, bias-aware AI, and accountable risk management. By unifying GDPR mandates with EU AI Act Article 10, embedding ISO/IEC 27701 PIMS, and leveraging the NIST Privacy Framework, DSIP ensures measurable, evidence-based protection of individuals' rights while enabling effective, compliant data use across programmes and jurisdictions.

Chapter 9 — Technology Operations & Secure DevSecOps

9.1 Purpose and Scope

This Chapter establishes DSIP's operational technology doctrine and secure-by-design engineering system for software and infrastructure. It defines the controls, processes, and evidence required to operate cloud-native stacks, CI/CD pipelines, and microservices securely; it mandates supply-chain integrity through SBOMs and attested builds; and it integrates the requirements for trustworthy AI systems (technical documentation, records, transparency, human oversight, accuracy, robustness, and cybersecurity) as prescribed by the EU AI Act. The Chapter aligns DSIP practices with the NIST Secure Software Development Framework (SSDF) SP 800-218, the NIST DevSecOps and microservices guidance (SP 800-204 series), OWASP SAMM and OWASP ASVS, SLSA supply-chain levels, and hardening guidance for Kubernetes-based platforms issued jointly by NSA/CISA.

9.2 Secure-by-Design Engineering Mandate

DSIP adopts Secure by Design as an executive-level obligation: security outcomes for our constituents are owned by the manufacturer/provider, enabled by default configurations, and evidenced through transparent processes. This mandate follows the principles articulated by CISA and partner agencies and is binding across all DSIP technology programmes.

To operationalise this mandate, DSIP implements the NIST SSDF (SP 800-218) across the SDLC. SSDF provides a common vocabulary and high-level practices—organised around "Prepare," "Protect," "Produce," and "Respond"—that are integrated into DSIP's governance and procurement. The SSDF reduces vulnerability introduction, mitigates impact when defects remain, and addresses root causes to prevent recurrence; suppliers are required to attest to SSDF-conformant practices.

9.3 DevSecOps Architecture and Controls

9.3.1 Reference Architecture (Microservices, Service Mesh, CI/CD)

DSIP's cloud-native architecture uses microservices (often containerised) orchestrated by Kubernetes, with secure service-to-service interactions enforced via a service mesh (e.g., mutual TLS, policy-as-code, and zero-trust runtime policies). NIST's SP 800-204A and SP 800-204C guide our deployment and DevSecOps primitives—continuous integration, delivery, deployment, and feedback—implemented as code (application code, services code, infrastructure-as-code, policy-as-code, observability-as-code) to achieve continuous authority to operate.

9.3.2 Kubernetes Platform Hardening

DSIP platforms comply with the NSA/CISA Kubernetes Hardening Guidance (v1.2), including least-privilege pods, network separation, strong authentication and RBAC, audit logging, vulnerability scanning of containers/pods, and regular configuration review and patching. The guidance addresses data theft, resource hijacking, and denial-of-service risks typical in container environments and prescribes isolation of control-plane components.

9.3.3 Application Security Verification

All DSIP applications are verified against OWASP ASVS v5.0.0 requirements appropriate to assurance level (typically Level 2, Level 3 for high-value or safety-critical services). ASVS normalises technical control coverage for web apps and APIs and provides testable requirements for authentication, session management, access control, input validation, cryptography, logging, data protection, and configuration.

9.3.4 Programme Maturity and Governance

DSIP measures secure development maturity using OWASP SAMM v2, across Governance, Design, Implementation, Verification, and Operations. SAMM supports risk-driven, iterative improvement, with assessments, benchmarks, and defined activities to demonstrate concrete progress in programme capability.

9.4 Software Supply-Chain Integrity

9.4.1 SBOMs (Minimum Elements) and Formats

Every DSIP release (and third-party software used in DSIP stacks) shall include an SBOM meeting the NTIA Minimum Elements—data fields (supplier, component, version, unique identifiers, dependency relationships, author, timestamp), automation support, and documented practices/processes—suitable for machine processing and lifecycle use.

SBOMs must be provided in a recognised open standard: SPDX (ISO/IEC 5962:2021; v2.2.1/2.3; v3 profiles for expanded security and VEX relationships) and/or CycloneDX (ECMA-424) with support for SBOM/VEX, SaaSBOM, HBOM, ML-BOM, and cryptography BOM.

DSIP monitors the 2025 update to Minimum Elements published for comment by CISA and will incorporate finalised changes—e.g., explicit component hash, license fields, generation context, tool provenance—into SBOM generation and exchange processes.

9.4.2 Build Integrity and Provenance (SLSA)

All DSIP artefacts are built to SLSA levels appropriate to risk, with a roadmap to Level 3 across core systems. At minimum, DSIP requires automated builds with signed provenance (Build L2) and hardened build platforms resisting tampering during the build (Build L3), enabling verification that the artefact was built as expected.

9.4.3 CI/CD Controls

CI/CD pipelines enforce SSDF-consistent controls: code protection (restricted access and tamper-evident repositories), build integrity verification, release component archiving, vulnerability scanning (SCA/SAST/DAST/Container), and secure secrets management. These practices are directly drawn from SSDF's "Protect" and "Produce" categories and mandated in supplier attestations.

9.5 AI Systems: Technical Operations and Compliance

For DSIP deployments of high-risk AI systems, operations must satisfy the EU AI Act's technical obligations, integrated into DevSecOps evidence bundles:

- **Technical Documentation (Art. 11)** and **Record-Keeping (Art. 12):** comprehensive technical files, versioned telemetry, and reproducible build artefacts, aligned to SBOM and SLSA provenance.
- **Transparency and Information to Deployers (Art. 13):** operational disclosures and guidance, integrated into release notes and deployment runbooks.
- **Human Oversight (Art. 14):** controls ensuring meaningful human intervention, override capability, and monitoring tasks embedded in operations ("policy-as-code," "observability-as-code").
- **Accuracy, Robustness, and Cybersecurity (Art. 15):** model performance monitoring, adversarial testing, and cybersecurity measures commensurate with risk; dataset governance per **Article 10** (quality, representativeness, bias detection and mitigation).

9.6 Operational Runbooks and Evidence

9.6.1 Platform Hardening Runbook

- Enforce pod security standards; disable automounting of service account tokens unless necessary; implement least-privilege RBAC; segment networks to isolate kubelet and control-plane; enable audit logging; and continuously scan images/pods for vulnerabilities or misconfigurations. Evidence includes configuration baselines, audit logs, and scan reports per NSA/CISA guidance.

9.6.2 Application Verification Runbook

- Map critical applications to **ASVS** levels and chapters; define test coverage and remediation SLAs; maintain verification reports and defect management logs as part of release checklists.

9.6.3 SBOM and Build-Provenance Runbook

- Generate SBOMs at build time (SPDX and/or CycloneDX); sign artefacts and provenance; publish SBOMs with releases; maintain discovery and access channels to allow consumers to fetch machine-readable SBOMs; record tool versions and generation context in the SBOM.

9.6.4 DevSecOps Evidence Pack

- Maintain SSDF implementation matrices, CI/CD control attestations, vulnerability reports, pen-test/verification outcomes, SLSA level declarations, and AI Act technical documentation.

9.7 Metrics and MRV (Measurement, Reporting, Verification)

DSIP tracks:

1. **SSDF Adoption:** % of products with SSDF practices fully implemented (Prepare/Protect/Produce/Respond) and supplier attestations received; audit sampling outcomes. [csrc.nist.gov]

2. **ASVS Conformance:** proportion of applications at Level 2/Level 3; number of ASVS controls verified per release cycle; remediation SLAs.
3. **Kubernetes Hardening Compliance:** control-plane isolation, pod-security violations per thousand pods, audit-log coverage, patch latency.
4. **Supply-Chain Integrity:** SLSA levels achieved per artefact; % releases with signed provenance; SBOM completeness per NTIA/CISA minimum elements.
5. **AI Act Technical Operations:** completeness of technical documentation and record-keeping (Arts. 11–12), oversight controls (Art. 14), transparency guidance (Art. 13), and robustness/cybersecurity testing (Art. 15).

9.8 Closing Statement

This Chapter codifies DSIP's technology operations as a secure-by-design, audit-ready system. By embedding SSDF practices into DevSecOps, hardening cloud-native platforms per NSA/CISA guidance, verifying applications with OWASP standards, and enforcing supply-chain integrity through SBOMs and SLSA, DSIP maintains lawful, resilient operations. Integrating EU AI Act obligations ensures that DSIP's AI deployments remain accurate, robust, transparent, and subject to meaningful human oversight, with verifiable documentation and records

Chapter 10 — Transparency, Communications, and Public Reporting

10.1 Purpose and Scope

This Chapter defines DSIP's binding transparency and communications regime for disclosures to data subjects, deployers, regulators, partners, and the public, with auditable records that meet privacy law, AI transparency mandates, and incident-reporting standards. It operationalises transparency principles from the OECD Privacy Guidelines (including openness and accountability), the GDPR information duties (Articles 13 and 14), breach notification and data-subject communication (Articles 33 and 34), and the EU AI Act transparency obligations applicable to high-risk and certain other AI systems, and aligns incident communications with NIST SP 800-61 Rev. 3.

10.2 Transparency Principles and Legal Basis

10.2.1 Openness and Accountability

DSIP adopts OECD's eight privacy principles—specifically openness (a general policy of openness about developments, practices, and policies with respect to personal data) and accountability (the controller's responsibility for compliance)—as baseline commitments for public transparency statements and evidence registers. [oecd.org]

10.2.2 Information to Data Subjects (Privacy Notices)

When DSIP collects personal data directly, the privacy notice must include, at collection time, the controller identity and contacts, DPO contacts (where applicable), purposes and legal basis, legitimate interests (if relied upon), categories of recipients, and third-country transfer information and safeguards; additional information must cover retention, rights (access, rectification, erasure, restriction, objection, portability), consent withdrawal, complaint rights, whether provision is mandatory, and existence of automated decision-making including meaningful information on the logic and envisaged consequences.

Where personal data are obtained from sources other than the data subject, DSIP provides equivalent information, including categories of data, source of data (including whether publicly accessible), and the items above necessary for fair and transparent processing.

10.3 AI Transparency and Public Disclosures

10.3.1 High-Risk AI Systems (Deployers' Instructions and Transparency)

For high-risk AI, DSIP ensures the operation is sufficiently transparent to enable deployers to interpret outputs appropriately, accompanied by instructions that are concise, complete, correct, and clear, covering identity/contacts, intended purpose, expected accuracy metrics, robustness and cybersecurity information, conditions affecting performance, risks under intended or reasonably foreseeable misuse, explainability capabilities, input-data specifications, human oversight measures, computational/hardware requirements, expected lifetime, maintenance and logging, and any pre-determined changes to performance.

10.3.2 Transparency for Certain AI Systems (Public-Facing Interactions and Synthetic Content)

Where DSIP deploys AI intended to interact directly with natural persons, individuals must be informed they are interacting with an AI system unless obvious; providers of AI (including general-purpose AI) that generate synthetic audio, image, video or text ensure outputs are marked in a machine-readable format and detectable as artificially generated or manipulated; deployers of emotion recognition or biometric categorisation inform exposed persons of the operation; deployers of “deep fake” content disclose that content has been artificially generated or manipulated, subject to limited legal exceptions.

10.4 Incident Communications and Breach Reporting

10.4.1 Supervisory Authority Notification

In case of a personal data breach, DSIP notifies the competent supervisory authority without undue delay and, where feasible, no later than 72 hours after becoming aware, unless the breach is unlikely to result in a risk to rights and freedoms; where notification occurs after 72 hours, reasons for delay are provided, and the notification includes, at minimum, the nature of the breach (including affected categories and approximate numbers), DPO or contact details, likely consequences, and measures taken or proposed to address and mitigate adverse effects.

10.4.2 Communication to Data Subjects

When a breach is likely to result in a high risk to natural persons, DSIP communicates the breach to data subjects without undue delay in clear and plain language, describing the nature of the breach, likely consequences, and measures taken or proposed; communication may be omitted if appropriate technical and organisational measures rendered data unintelligible (e.g., effective encryption), if subsequent measures remove high risk, or if individual communication would involve disproportionate effort, in which case DSIP issues an effective public communication.

10.4.3 Incident Response Messaging (NIST SP 800-61 Rev. 3)

Incident communications are integrated across CSF 2.0 Functions—Govern, Identify, Protect, Detect, Respond, Recover—to ensure clear roles, prepared templates, evidence capture, stakeholder coordination, and continuous improvement using lessons learned; DSIP references NIST's Revision 3 recommendations for risk-aligned incident response activities and public messaging.

10.5 Vulnerability Disclosure and Security Advisories

DSIP maintains a coordinated vulnerability disclosure programme consistent with ISO/IEC 29147:2018, with defined intake channels, triage, remediation communication, and advisory publication, enabling users to perform technical vulnerability management and reduce exploitation risk; communications include remediation information, timelines, and, where multiple vendors are affected, coordinated releases.

10.6 Software Bill of Materials (SBOM) Publication and Access

To strengthen supply-chain transparency, DSIP publishes machine-readable SBOMs for DSIP software in recognised open formats (SPDX and/or CycloneDX) and ensures they meet NTIA Minimum Elements—data fields, automation support, and practices/processes—providing discoverability and updates; DSIP monitors CISA's 2025 draft update to Minimum Elements and will incorporate final changes once adopted.

10.7 Communications Governance and Channels

10.7.1 Authorised Channels

All external communications are issued through authorised channels: (i) privacy notices and public transparency pages; (ii) security advisories and CVE notices; (iii) SBOM portals or registries; (iv) incident notices to authorities and data subjects; and (v) AI transparency notices and content labelling. Each channel maintains versioned records for audit and evidence. (Privacy and breach communications per GDPR Articles 13/14/33/34; AI notices per AI Act Articles 13 and 50.)

10.7.2 Message Content Standards

Message content adheres to legal specifics (e.g., clear articulation of controller identity, rights, risks, and measures) and technical transparency (e.g., AI instructions and labelling), with plain-language summaries and structured annexes where appropriate (GDPR and AI Act).

10.8 Public Reporting and MRV (Measurement, Reporting, Verification)

10.8.1 Transparency Reports

DSIP issues periodic public transparency reports that enumerate: (i) privacy notice changes and DPIA volumes; (ii) breach notifications (aggregated counts, categories, timeliness); (iii) vulnerability advisories and remediation SLAs; (iv) SBOM coverage and update cadence; and (v) AI transparency metrics (e.g., proportion of labelled synthetic content, instructions distribution to deployers). The report references OECD openness/accountability, GDPR reporting obligations, and AI Act transparency sections.

10.8.2 KPIs and Evidence

Mandatory KPIs include:

- **Privacy Notice Compliance:** % of services with Article 13/14-compliant notices; audit findings.
- **Breach Reporting Timeliness:** proportion notified ≤72 hours; reasons for delay; data-subject communication timeliness.
- **CVD Performance:** mean time-to-acknowledge and time-to-remediate per ISO/IEC 29147.
- **SBOM Coverage:** % releases with NTIA-conformant SBOMs and consumer access; adoption of any **CISA 2025** enhancements once finalised.
- **AI Transparency:** % of deployers receiving complete instructions (Article 13); % of synthetic outputs correctly labelled (Article 50).

Evidence packs include versioned notices, advisory texts, SBOM files, logs of AI content labelling, regulator submissions, and communications playbooks aligned with NIST SP 800-61r3.

10.9 Records Management and Auditability

All communications (privacy notices, AI instructions, breach notifications, advisories, SBOM publications) are preserved with timestamps, authorship, and distribution records to enable supervisory verification and public accountability; breach communications are documented to enable authorities to verify compliance (GDPR Articles 33–34).

10.10 Closing Statement

By codifying openness and accountability, DSIP provides clear privacy information at collection and beyond, labels and explains AI systems in line with the EU AI Act, discloses incidents promptly with regulator and data-subject messaging, coordinates vulnerability remediation, and publishes SBOMs for supply-chain transparency. Public reporting with MRV enforces trust and legal conformity while enabling continuous improvement across programmes and jurisdictions

Chapter 11 — Operations Security & Resilience (Business Continuity and Disaster Recovery)

11.1 Purpose and Scope

This Chapter establishes DSIP's enterprise-wide Business Continuity and Disaster Recovery (BC/DR) framework and the operational safeguards required to sustain essential services during disruptive events, restore normal operations in a controlled manner, and evidence compliance to partners and authorities. The framework aligns with NIST SP 800-34 Rev. 1 for information system contingency planning and the NIST SP 800-184 recovery guidance for cybersecurity events, and is harmonised with DSIP's incident response Chapter and CSF 2.0 governance and improvement cycles.

11.2 Resilience Governance

11.2.1 Policy and Organisational Roles

DSIP's Resilience Policy mandates a documented BC/DR programme integrated with operations, security, and risk management. The governance model assigns clear responsibilities to the Continuity Lead, System Owners, and the CSIRT for coordination across preparation, response, recovery, and continuous improvement. This is consistent with the management and lifecycle approach described in SP 800-34 Rev. 1.

11.2.2 Integration with Incident Response and CSF 2.0

Resilience activities are mapped to CSF 2.0 Functions—Govern/Identify/Protect supporting Detect/Respond/Recover—and incorporate lessons learned to strengthen controls and continuity postures, as recommended in SP 800-184 and the incident response profile in SP 800-61 Rev. 3.

11.3 Business Impact Analysis (BIA)

11.3.1 Critical Functions and Dependencies

Each DSIP service conducts a BIA to identify critical business functions, supporting systems, facilities, suppliers, data repositories, and regulatory reporting obligations. The BIA establishes Maximum Tolerable Downtime (MTD), Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and inter-service dependencies in accordance with SP 800-34 Rev. 1.

11.3.2 Risk Scenarios and Impact Categories

Risk scenarios (e.g., ransomware, cloud region failure, supply-chain outage, loss of identity provider) are analysed for operational, legal, safety, reputational, and financial impacts. The BIA informs prioritisation of recovery strategies and resource allocations as contemplated by SP 800-34 Rev. 1.

11.4 Continuity and Recovery Strategies

11.4.1 Technical Recovery Strategies

Recovery strategies must be commensurate with MTD/RTO/RPO and include:

- **Data protection and restore:** robust back-up regimes with off-site/immutable storage; documented restore procedures and verification in line with SP 800-184's recovery playbooks.
- **Redundancy and failover:** multi-region or multi-availability-zone deployment, active/active or active/passive failover, and warm/cold standby patterns per the contingency planning guidance in SP 800-34 Rev. 1.
- **Configuration and infrastructure as code (IaC):** version-controlled baseline configurations and automated rebuild, consistent with SP 800-184's emphasis on rapid restoration using pre-approved playbooks.

11.4.2 Organisational Continuity Strategies

- **Alternative sites and work areas:** arrangements for alternate locations and secure remote operations, including telework procedures and communication measures per SP 800-34 Rev. 1.
- **Supplier/third-party continuity:** contractual clauses requiring incident cooperation, forensic access (as covered in Chapter 9's supply-chain) and continuity support; DSIP validates supplier recovery capabilities during onboarding and periodic reviews. (Cross-references to Chapter 9; see Kubernetes/DevSecOps and SBOM measures.)

11.5 Cybersecurity Event Recovery

11.5.1 Recovery Playbooks

For cyber events, DSIP maintains system-specific Recovery Playbooks that specify:

- Preconditions and triggers for initiating recovery.
- Authority to invoke and escalation paths.
- Restoration sequencing and dependency checks.
- Data validation, integrity assurance, and cryptographic verification.
- Communication templates for internal/external stakeholders.

These playbooks follow the tactical and strategic guidance in SP 800-184, with emphasis on testing, metrics, and continuous improvement.

11.5.2 Breach Notification and Communications

Recovery activities are coordinated with legal communications under GDPR Articles 33 and 34 (72-hour supervisory authority notification; clear data-subject communication where high risk exists) and with CSIRT messaging aligned to SP 800-61 Rev. 3.

11.6 Plan Development and Documentation

11.6.1 Plan Components

Each system's Information System Contingency Plan (ISCP) contains:

- Statement of importance, assumptions, and roles/responsibilities.
- BIA summary with recovery priorities.
- Preventive controls and continuity strategies.
- Detailed recovery procedures and validation steps.

- Alternate processing and data restoration procedures.
- Communications plan (regulatory, customer/partner, media).
- Plan maintenance and version-control procedures.

This structure is consistent with the plan elements outlined in **SP 800-34 Rev. 1**.

11.6.2 Evidence and Records

Plans, exercises, test results, after-action reports, and corrective actions are preserved to demonstrate adherence to SP 800-34 Rev. 1 and SP 800-184.

11.7 Testing, Training, and Exercises (TT&E)

11.7.1 Exercise Types and Frequency

DSIP executes an annual TT&E programme including table-top, functional, and full-interruption tests where feasible, and cyber-focused exercises using simulated ransomware and cloud-region loss scenarios. Exercise design, documentation, and post-exercise corrective actions follow the iterative improvement approach in SP 800-34 Rev. 1 and SP 800-184.

11.7.2 Training and Awareness

Operational teams receive role-specific training on recovery procedures, data validation, and coordinated communications; executives and continuity coordinators receive decision-making training on plan invocation thresholds and regulatory obligations (GDPR Articles 33–34).

11.8 Metrics and MRV (Measurement, Reporting, Verification)

11.8.1 KPI Families

- **Continuity Readiness:** % systems with current ISCPs; % staff trained; time since last exercise per system. (SP 800-34 Rev. 1 benchmarks.)
- **Recovery Performance:** mean time-to-restore vs. RTO; data-loss observed vs. RPO; restoration success rate and error/rollback counts. (SP 800-184 metrics guidance.)
- **Compliance Timeliness:** breach notifications within 72 hours; data-subject communications timeliness; documentation completeness (GDPR).
- **Improvement Loop:** # of corrective actions closed per quarter; exercise-derived control changes implemented (SP 800-184, CSF 2.0 Improvement).

11.8.2 Reporting Cadence

Quarterly resilience reports to governance bodies include KPI results, significant findings, remediation tracking, and resource requests; annual public transparency report summarises exercise volumes and recovery outcomes at an appropriate aggregation level (Chapter 10).

11.9 Dependencies and Cross-References

This Chapter should be read together with:

- **Chapter 7 (Operational Security & Incident Response):** for incident lifecycle, evidence preservation, and forensic coordination (SP 800-61 Rev. 3).
- **Chapter 9 (Technology Operations & Secure DevSecOps):** for platform hardening and automated rebuild (service mesh, IaC), which materially improves recovery reliability (SP 800-204A/C; NSA/CISA Kubernetes).

- **Chapter 10 (Transparency, Communications, and Public Reporting):** for breach communications content and public reporting, aligned to GDPR and AI transparency mandates.

11.10 Closing Statement

DSIP's BC/DR architecture is a disciplined, standards-anchored system that safeguards essential services under stress and restores operations with documented assurance. By applying SP 800-34 Rev. 1 for contingency planning and SP 800-184 for cyber event recovery—and integrating incident response and transparency processes—DSIP maintains lawful, resilient, and auditable operations across programmes and jurisdictions

Chapter 12 — Quantitative Broadband-Usage Analysis and Capacity Volumetrics

12.1 Purpose and Scope

This Chapter sets out the definitive quantitative methodology and volumetrics for DSIP transport and metropolitan networks, expressed in daily, monthly, and annual data movement. The approach follows recognised international teletraffic engineering practice and ITU business planning methods; it integrates sectoral drivers (education, households, public administration, SMEs) and platform-specific bandwidth guidance to ensure that capacity projections are defensible, auditable, and suited to AfDB due diligence.

12.2 Methodology and Core Assumptions

DSIP applies the ITU ICT Infrastructure Business Planning Toolkit for economic and traffic modelling and the ITU-T E-series principles for teletraffic measurement (offered/carried traffic, busy-hour dimensioning, peak-to-average conversion). The backbone is engineered to a busy-hour (BH) line-rate of approximately 1.6 Tbps, derived from concurrency and bitrate assumptions established for education, household streaming, public administration collaboration, and SME usage. In line with global observations that busy-hour grows more rapidly than average traffic, DSIP converts BH to average sustained load using a conservative factor of average ≈ 20% of BH. This choice reflects the empirically observed gap between peak and mean loads (busy-hour increasing ~4.8× versus average ~3.7× over 2017–2022) and avoids underestimation of transport volumes.

12.3 Capacity Volumetrics (Daily, Monthly, Annual)

Using the engineered BH capacity and the 20% conversion ratio, DSIP's average sustained load is **0.32 Tbps (320 Gbps)**. Converting line-rate to volumes:

- **Daily:** ~3.46 PB/day
- **Monthly (30 days):** ~103 PB/month
- **Annual:** ~1.25 EB/year

The conversions follow SI network units and standard bit-to-byte transformations recognised in teletraffic work and operator planning.

Table 12-A: Capacity and Volume Summary

Metric	**Value**	**Equivalent**
Busy-hour line-rate	**1.6 Tbps**	**200 GB/s**

Metric	Value	Equivalent
Average sustained load (20%)	**320 Gbps**	**40 GB/s**
Data per hour (average)	**~144 TB/h**	**0.144 PB/h**
Data per day (average)	**~3.46 PB/day**	**~3,456 TB/day**
Data per month (30 days)	**~103 PB/month**	**~103,680 TB/month**
Data per year	**~1.25 EB/year**	**~1,244 PB/year**

Computation note: 320 Gbps ÷ 8 = 40 GB/s; × 3,600 s = 144,000 GB ≈ 144 TB/h; × 24 = ~3.46 PB/day; × 30 = ~103 PB/month; × 12 = ~1.25 EB/year.

12.4 Sectoral Drivers and Contribution Rationale

The aggregate DSIP volumes reflect simultaneous carriage of multi-sector traffic:

1. **Education connectivity.** DSIP sizes school external links to the FCC's goal of ≥ 1 Mbps per student, which yields substantial concurrent loads during school-day peaks; national progress toward 1 Gbps per 1,000 students/staff benchmarks underscores the scale.

2. **Household streaming and live platforms.** Streaming dominates consumer busy-hour: measured Netflix usage ranges from ~1 GB/h (SD) to ~7 GB/h (4K), implying ~3–5 Mbps for 1080p and ~15 Mbps for 4K; YouTube Live recommends ~10–12 Mbps for 1080p and ~30 Mbps for 4K ingest. DSIP's BH design assumes a realistic share of households streaming concurrently.

3. **Collaboration traffic (public administration and SMEs).** HD meetings operate at ~3–4 Mbps per concurrent participant for Zoom/Teams, imposing predictable peaks for national and routine events.

4. **Busy-hour engineering and headroom.** The model embeds diversity and safety margins consistent with ITU toolkits and operator best practice, ensuring resilience across inter-city spans and cross-border routes.

Illustrative Contribution (pre-buffer raw BH):

Segment	Raw BH (Gbps)	Share of BH (%)	Primary driver
Education (K-12)	~400	~38.8%	FCC ≥ 1 Mbps per student; school concurrency
Households	~320	~31.1%	Netflix/YouTube bitrates; household streaming
SMEs	~210	~20.4%	HD collaboration; SaaS
Public administration	~100	~9.7%	HD collaboration; data sharing
Total	**~1,030**	**100%**	–

Comparative note (health-specific programmes). Sector-specific initiatives in health typically present smaller volumetrics (e.g., ~64 PB/year in indicative low-calculation health enablement contexts) because scope is narrower, concurrency is limited to professional cohorts, and traffic seldom includes mass-market streaming or the FCC per-student guarantees. DSIP, as the general-purpose national backbone, must accommodate peak education loads, consumer streaming, and nationwide collaboration simultaneously, which inflates BH and, therefore, monthly/annual volumes.

12.5 Sensitivity and Scenario Analysis

DSIP volumetrics respond predictably to changes in application mix and concurrency:

- **Shift toward 4K streaming.** If the 4K share increases (15 Mbps per stream vs ~5 Mbps for 1080p), household BH grows proportionally and monthly volumes exceed ~103 PB.
- **National conferencing events.** Elevated concurrent participants at ~3–4 Mbps per user increase collaboration BH; buffering and QoS must preserve service quality.
- **Lower school-day concurrency.** If active student ratios reduce, education BH moderates; however, the FCC target still anchors per-student capacity obligations.

Global traffic studies corroborate that device proliferation and content shifts widen the gap between busy-hour and daily averages, warranting cautious dimensioning for multi-year horizons.

12.6 Visualisation Tables (Units and Application Anchors)

Table 12-B: Unit Conversions (network/storage)

Quantity	**Decimal (network, SI)**	**Binary (storage, IEC)**
1 Gb	10^9 bits	2^30 bits (≈ 1.074×10^9)
1 TB	10^12 bytes	2^40 bytes (≈ 1.099×10^12)
1 PB	10^15 bytes	2^50 bytes (≈ 1.126×10^15)

(*Use SI for line-rates and volumes; IEC may be applied for storage subsystems.*)

Table 12-C: Application-Level Consumption (Design Anchors)

Service / Mode	**Typical bitrate (Mbps)**	**Data / hour (GB)**
Netflix – 1080p	~5	~2.3–3.0
Netflix – 4K	~15	~6.5–7.0
YouTube Live – 1080p30	~10	~4.5–5.0
YouTube Live – 4K30	~30	~13.5–15.0
Zoom/Teams — HD participant	~3–4	~1.4–1.8 (effective)

12.7 Engineering and Procurement Implications

Transport procurement must anticipate multi-Tbps per route with modular upgrades (DWDM with coherent 400G/800G, ROADM flexibility, C+L band scaling). IP/MPLS layers should be sized to average load plus safety margin, with QoS profiles that prioritise real-time collaboration and critical public-service traffic. The AfDB portfolio context—long-distance cross-border fibre segments and national data centres—aligns with such multi-Tbps scalability and resilience design.

12.8 Compliance and Evidentiary Basis

This Chapter provides AfDB-ready volumetrics and sectoral drivers supported by authoritative sources. The methodology is grounded in ITU planning toolkits and teletraffic principles, incorporates FCC education connectivity standards, and references platform-specific bitrate guidance for streaming and collaboration services. Global traffic forecasts and busy-hour growth dynamics substantiate the capacity envelope. These evidentiary anchors ensure that DSIP's projected volumes—approximately 103 PB per month and 1.25 EB per year—are aligned with international best practice and suitable for audit and validation.

Chapter 13 — Closing Statement

The DESA Security & Integrity Program (DSIP) constitutes a sovereign, ethical, and scalable security architecture designed to safeguard digital ecosystems across all sectors of national development. It integrates lawful data governance, algorithmic transparency, accessibility, and fiduciary integrity into a unified operational framework that is auditable and aligned with international standards.

Through its layered architecture—Infrastructure, Application, and Capacity—DSIP enforces compliance with GDPR, the African Union Data Policy Framework, and regional harmonisation instruments under COMESA, SADC, and EAC. It embeds ethical AI principles and accessibility baselines (WCAG 2.2, EN 301 549), ensuring inclusivity and trust in all public-facing services. Technical operations adopt secure-by-design engineering, DevSecOps practices, and supply-chain integrity measures (SSDF, SBOM, SLSA), while resilience is guaranteed through business continuity and disaster recovery protocols anchored in NIST SP 800-34 and SP 800-184.

The programme's fiduciary architecture leverages blended finance and PPP frameworks consistent with AfDB guidance, incorporating affordability safeguards and tariff covenants to uphold social equity. Measurement, Reporting, and Verification (MRV) systems provide transparent dashboards, independent audits, and grievance redress pathways, reinforcing accountability at every tier.

Quantitative analysis confirms DSIP's strategic role as the backbone for national and regional digital transformation: engineered for multi-terabit capacity, capable of moving ~103 PB per month and ~1.25 EB annually, with scalability to meet projected growth trajectories. These volumes reflect DSIP's mandate to serve education, public administration, SMEs, and households concurrently, ensuring compliance with international connectivity standards and readiness for emerging digital services.

In delivering this architecture, DSIP positions itself as a cornerstone of DESA's long-term vision—a lawful, ethical, and resilient digital foundation that strengthens national competitiveness, accelerates socio-economic inclusion, and aligns with continental and global agendas, including Agenda 2063, Agenda for Social Equity 2074, and AfDB's High-5 priorities. It is not merely a technical programme; it is a governance instrument for trust, transparency, and sustainable growth.