DECEMBER 18, 2025

# PCDE — CHARTER & OPERATING MANUAL

*Constitutive Instrument for Governance, Compliance, and Fiduciary Architecture of the Pan-Continental Digitalisation & Equity Programme*

**CREATED BY**
EUSL AB
*Care to Change the World*

# Table of Contents

# PCDE— Charter & Operating Manual

## Introduction

This Charter & Operating Manual gives legal effect and operational guidance to the PCDE Legacy Project as described in Document 1, consolidating its juridical status, mandate, institutional organs, decision rights, and compliance canon. It adopts open and internationally recognized standards for procurement transparency, financial reporting, cybersecurity, and development finance disclosure to ensure credibility with member states, development finance institutions, and private investors. For avoidance of doubt, the Charter aligns implementation to the African Union's Digital Transformation Strategy (2020–2030), the African Development Bank's "High 5" priorities, and, where applicable, the COMESA-coordinated IDEA multiphase programmatic approach, without derogation from national legal orders or treaty obligations.

## Chapter One — Establishment, Legal Personality, Seat

**Establishment**

PCDE is hereby established as a constitutive programme and operating regime for digitalisation and equity, authorized to constitute or designate one or more implementing legal entities (each, a "PCDE Entity") in participating jurisdictions for the purposes of contracting, financial management, asset holding, and staff engagement. Each PCDE Entity shall be incorporated under the relevant host-state law or under an intergovernmental instrument, as determined by resolution of the Governing Council, and shall operate under this Charter and any Host Country Agreement, without prejudice to mandatory rules of the host legal order. The establishment framework is designed to interlock with regional integration programmes, including the AU Digital Transformation Strategy and, where relevant, the COMESA-coordinated IDEA platform.

**Legal Personality and Capacity**

Each duly constituted PCDE Entity possesses separate legal personality with full capacity, within its jurisdiction of establishment, to contract, acquire and dispose of movable and immovable property, open and operate bank and custody accounts, hire personnel, issue and receive grants and loans, sue and be sued, and otherwise perform acts necessary for the execution of PCDE's mandate. Where a Host Country Agreement or intergovernmental instrument confers privileges and immunities, such arrangements shall be strictly limited to functional necessity and shall not shield acts ultra vires or contrary to the Charter's compliance and integrity obligations. PCDE's financial statements and asset registers shall be prepared on an accrual basis consistent with International Public Sector Accounting Standards (IPSAS), with transition reliefs for first-time adoption applied in accordance with prevailing IPSASB guidance and handbooks.

**Seat and Offices**

The Governing Council shall designate the principal seat by resolution, taking into account host-state commitments to PCDE's compliance canon, digital policy alignment with the AU strategy, and regional coordination needs. The Secretariat may maintain regional or country offices to support corridor deployments, Digital Education & Innovation Centres (DEICs), and trust-service nodes. In the COMESA region, co-location or structured coordination with IDEA program units is permitted to avoid duplication and to benefit from harmonised corridor planning, skills development, and regional market integration.

### Seat and Jurisdiction Architecture (indicative)

| Office Type | Purpose | Jurisdictional Instrument | Minimum Compliance Commitments |
|---|---|---|---|
| Principal Seat (Secretariat) | Central governance, policy, standards custody, inter-REC coordination | Host Country Agreement or not-for-profit/incorporated entity under host law | IPSAS financial statements; OCDS procurement disclosure; IATI activity reporting; ISO/IEC 27001 ISMS; NIST SP 800-207 Zero-Trust controls for information assets. |
| Regional Office | Corridor planning, DEIC support, vendor/pre-market engagement | Registration under host law or MoU with REC secretariat | Alignment to AU DTS pillars and REC programmes; publication of project datasets to OCDS/IATI. |
| Country Office / Project SPV | Local contracting, permits, asset operations, PPP interface | Special purpose vehicle or branch registration | Host-state fiduciary compliance; IPSAS accrual reporting; open contracting data release. |

## Chapter Two — Mandate, Functions, Duration

**Mandate**

PCDE's mandate is to design, finance, and operate modular digitalisation interventions that combine open-access fibre corridors, DEIC nodes, AI-enabled public services, and verifiable trust-service rails, with a view to inclusive growth, market activation, and public-sector service modernisation. The mandate is anchored to Agenda for Social Equity 2074, aligned to the AU Digital Transformation Strategy's pillars on infrastructure, skills, digital ID/trust, cybersecurity, and data governance, and supportive of the AfDB "High 5" priorities—particularly "Integrate Africa," "Improve the Quality of Life," and "Industrialize/Feed Africa" where digital rails catalyse sector outcomes. In Eastern and Southern Africa, PCDE may be embedded or interoperable with the COMESA-coordinated IDEA multiphase program, provided that PCDE's compliance canon remains intact.

**Core Functions**

PCDE shall perform the following functions in furtherance of its mandate, subject to Governing Council oversight and the Delegations Framework established under this Charter:

1. **Programme Design and Corridor Activation.** Identify and structure cross-border and national backbone routes, IXPs, last-mile enablers, and DEIC nodes, using transparent, least-cost planning and harmonised regional toolkits where available. In COMESA jurisdictions, coordination with IDEA's regional planning and knowledge platforms is encouraged to avoid fragmentation and to accelerate scale.

2. **Open and Compliant Procurement.** Conduct all procurement using the Open Contracting Data Standard, publishing machine-readable tender, award, and contract implementation data and

documents and maintaining persistent identifiers to enable public scrutiny, competition, and value-for-money analysis.

3. **Fiduciary Management and Public Reporting.** Maintain accrual-basis financial statements in accordance with IPSAS; disclose budget-to-actual variances; and implement first-time adoption reliefs where necessary. PCDE shall publish development-finance flows, activity results, and forward plans using the International Aid Transparency Initiative (IATI) Standard to facilitate donor interoperability and external validation.

4. **Cybersecurity, Data Protection, and Trust Services.** Operate an information security management system aligned to ISO/IEC 27001 and implement a Zero-Trust Architecture consistent with NIST SP 800-207 and related practice guides, including identity, device, and workload trust brokerage across on-premises and multi-cloud environments.

5. **Results Measurement and Public Dashboards.** Integrate MEL with public dashboards that surface outcome indicators for access, adoption, governance, and market activation, ensuring linkages to AfDB "High 5" thematic outcomes and the AU strategy's digital inclusion and service delivery pillars.

6. **Policy Harmonisation and Regional Interlocks.** Where appropriate, align corridor and node operations with REC-level initiatives that address roaming, cross-border data flows, digital payments interoperability, and unified standards for cybersecurity and e-trust services; this includes collaboration with COMESA on regional digital market integration initiatives and related EU-supported programmes aimed at secure cross-border e-commerce and payments.

**Duration**

The Charter enters into force upon adoption by the founding resolution and remains effective through the 2026–2074 programme horizon, with quinquennial strategic reviews to confirm mandate fitness, update compliance references to later versions of international standards, and adjust institutional arrangements as necessary. The Governing Council may extend, suspend, or terminate the Charter pursuant to the procedures set out in later chapters of this instrument, without prejudice to accrued rights or obligations under applicable law and financing agreements. The duration construct is calibrated to the AU Digital Transformation Strategy's 2030 horizon and the longer Agenda 2074 horizon, while maintaining interoperability with MDB program cycles and REC-level frameworks.

**References**


- **African Union — Digital Transformation Strategy (2020–2030).** AU DTS (official documents page).
- **African Development Bank — High 5 Priorities.** AfDB "High 5s" overview.
- **COMESA & World Bank — IDEA Programme.** World Bank Aide-Mémoire: Inclusive Digitalization for Eastern and Southern Africa (COMESA PCU); COMESA consultancy notice for least-cost digital infrastructure planning under IDEA.
- **Open Contracting Data Standard.** OCDS documentation (latest).
- **International Public Sector Accounting Standards.** IPSASB — official site; IPSASB Handbook 2024; Updated IPSAS 33 — first-time adoption notice.
- **IATI — International Aid Transparency Initiative.** IATI Standard and governance.

- **ISO/IEC 27001 — Information Security Management Systems.** ISO/IEC 27001:2022 overview.
- **NIST Zero Trust.** NIST SP 800-207 Zero Trust Architecture (final); NIST SP 1800-35 — Implementing a Zero Trust Architecture.
- **Regional Digital Market Facilitation (context).** EU–COMESA Safe Digital Boost Africa regional scoping workshop.

# Chapter Three — Organs: Governing Council, Executive Board, Secretariat

**Constitution of Organs**

PCDE is governed and administered through three principal organs established by this Charter: the Governing Council, the Executive Board, and the Secretariat. These organs act within the boundaries of applicable host-state law, this Charter, and the compliance canon, including open contracting and public-finance transparency standards and internationally recognized cybersecurity and information-security frameworks. The institutional architecture is designed to interface with regional digitalisation strategies (including the AU Digital Transformation Strategy and, where applicable, COMESA's IDEA platform) and to maintain credibility with development finance windows as articulated by the African Development Bank's strategic priorities.

**Governing Council**

The Governing Council is the supreme policy organ of PCDE. It sets strategic direction, adopts and amends the Charter and Operating Manual, approves the multi-year programme plan within the 2026–2074 horizon, and establishes the principal regulations, including Finance, Procurement, Safeguards, Data Protection, and Technology & Cybersecurity Regulations. The Council also designates the principal seat and authorizes the creation of regional and country offices. All Council actions shall be recorded and disclosed through public resolutions and, where relevant, integrated into open data publications consistent with the Open Contracting Data Standard (OCDS) and the International Aid Transparency Initiative (IATI) Standard to support external scrutiny and MDB interoperability.

Council membership, voting, and quorum are determined by adopted Council Standing Orders. Unless a qualified majority is expressly required by this Charter (e.g., Charter amendments, suspension, or termination), resolutions shall be approved by simple majority of members present and voting, provided quorum under the Standing Orders is met. Members shall uphold fiduciary neutrality and independence and are subject to the Conflict-of-Interest and Recusal Protocol described below.

**Executive Board**

The Executive Board is the corporate and operational decision organ charged with implementing Council policy and delivering programme outcomes. It approves annual operating plans, budgets, and financing structures; authorizes procurement and contracting within delegated thresholds; executes Host Country Agreements; and oversees performance of corridors, DEIC nodes, trust-service rails, and programme MEL dashboards. The Board ensures that accrual-basis financial statements are prepared under IPSAS, that first-time adoption reliefs are applied where appropriate, and that all development-finance flows and forward plans are published in IATI format for donor interoperability and accountability. Procurement processes and contract implementation data shall be published in machine-readable OCDS format, forming a continuous disclosure record from planning through award and delivery.

The Board shall maintain an approved Information Security Management System (ISMS) aligned to ISO/IEC 27001 and a Zero-Trust Architecture consistent with NIST SP 800-207 and related practice guides, covering identity, device, network, and workload trust policies across on-premises and multi-cloud environments. Cyber risk acceptance and residual risk registers are reviewed at each Board cycle and reported to the Council through the Compliance and Integrity Report.

**Secretariat**

The Secretariat is the administrative organ led by a Secretary-General (or equivalent title as determined by Council) and is responsible for day-to-day operations, programme preparation, stakeholder engagement, record-keeping, and publication of disclosures. The Secretariat houses functional units for Programme Design, Procurement & Contracting, Finance & Treasury, Safeguards & MEL, Data Protection & Cybersecurity, and Legal Affairs. It prepares annual financial statements in accordance with IPSAS, publishes all planned and actual procurement under OCDS, and releases activity data and results through IATI. The Secretariat ensures alignment of PCDE project portfolios to the AU Digital Transformation Strategy's pillars and the AfDB High-5 priorities, and, where appropriate, coordinates with COMESA's IDEA regional platforms on least-cost planning, skills development, and market integration.

**Compliance and Integrity Oversight**

Each organ shall cooperate with independent compliance audits covering financial statements, procurement integrity, and cybersecurity posture. Audits reference IPSAS for financial reporting, OCDS and procurement regulations for contracting transparency, IATI for aid-flow disclosures, ISO/IEC 27001 for ISMS conformance, and NIST SP 800-207 for Zero-Trust implementation maturity. Audit summaries and management letters are to be publicly disclosed, except for information properly classified under applicable data-protection law and security policies.

**Conflict-of-Interest and Recusal Protocol**

All members of the Governing Council, Executive Board, and senior Secretariat staff shall complete annual declarations of interest and file event-driven updates upon any change of circumstances. A member shall recuse from deliberations and abstain from voting on matters where a conflict exists or may reasonably be perceived, including direct or indirect financial interests, family or close personal ties to bidding entities, or prior employment relationships within the look-back period defined in the Procurement Regulation. Recusal events and abstentions shall be recorded in meeting minutes and disclosed in periodic integrity reports consistent with the OCDS implementation guidance concerning contracting-process transparency.

**Organ Interaction and Regional Interlocks**

The Secretariat shall submit quarterly performance reports to the Executive Board, including MEL dashboards and published datasets. The Board consolidates these into semi-annual Council Reports. In Eastern and Southern Africa, PCDE may interlock with the COMESA IDEA platform for harmonized corridor planning, capacity building, and regional market facilitation, provided that PCDE's Charter-mandated compliance canon remains intact and that disclosures are made through OCDS and IATI to maintain cross-donor comparability.

## Chapter Four — Decision Rights and Delegations

**Framework**

Decision rights and delegations are structured to ensure that strategic, fiduciary, and operational decisions are made at the appropriate level, with strong safeguards and public disclosure. The

Governing Council retains ultimate policy authority; the Executive Board exercises delegated corporate and operational authority; and the Secretariat executes within approved plans, budgets, and thresholds. All delegations are subject to the compliance canon, including IPSAS accrual reporting, OCDS procurement disclosure, IATI activity reporting, ISO/IEC 27001 ISMS controls, and Zero-Trust Architecture implementation.

**Decision Rights**

Strategic policies, Charter amendments, establishment of new offices, approval of multi-year programme plans, and adoption of principal regulations are reserved to the Governing Council. Approval of annual operating plans and budgets, authorization of financing structures (including sovereign and non-sovereign windows), sanctioning of major procurements and PPP frameworks, and oversight of cybersecurity posture are vested in the Executive Board, subject to thresholds and safeguards. Routine procurement and contracting, site permits, staffing, asset operations, MEL dashboards, and publication of disclosures are carried out by the Secretariat under Board-approved plans and within delegated limits. References to sovereign/non-sovereign windows reflect the AfDB's operational practice, which PCDE uses for interoperability with MDB co-financing and risk management.

**Delegations Matrix (normative structure; thresholds set by Finance & Procurement Regulations)**

| Decision Area | Authority | Delegated Authority | Threshold (indicative; to be set by regulation) | Mandatory Safeguards & Standards | Public Disclosure |
|---|---|---|---|---|---|
| Charter and Regulations (Policy) | Governing Council | None, except technical updates delegated to Board | N/A | Legal review; alignment to AU DTS and REC frameworks; conflict register | Publish resolutions; update Charter repository |
| Multi-Year Programme Plan (2026–2074) | Governing Council | Executive Board drafts | N/A | Alignment to AU DTS; AfDB High-5 outcomes mapping; MEL architecture | Publish plan, MEL logic models, IATI forward plans |
| Annual Budget and Operating Plan | Executive Board | Secretariat executes | Budget ceiling per Council approval | IPSAS accruals; internal controls; audit trail | Publish budget-to-actuals; IATI updates |
| Financing Structures (SO/NSO; PPPs) | Executive Board (within Council policy) | Secretariat negotiates within term sheets | Amount, tenor, and security caps set by Finance Regulation | Due-diligence memos; risk assessment; safeguards | Publish term sheets and financing summaries (subject to confidentiality) |

| Decision Area | Authority | Delegated Authority | Threshold (indicative; to be set by regulation) | Mandatory Safeguards & Standards | Public Disclosure |
|---|---|---|---|---|---|
| Procurement & Contracting | Executive Board (policy & major awards) | Secretariat (routine awards) | Tiered thresholds by lot value | OCDS publication; integrity checks; recusal | Full OCDS release from planning through implementation |
| Cybersecurity & Data Protection | Executive Board (policy & risk acceptance) | Secretariat (ISMS operations) | Risk acceptance thresholds as per Technology Regulation | ISO/IEC 27001 ISMS; NIST SP 800-207 ZTA | Publish policies and annual posture summaries |
| MEL and Public Dashboards | Executive Board (indicator set) | Secretariat (data operations) | N/A | Verification protocols; data quality controls | Publish dashboards; link to IATI activity results |
| Host Country Agreements & Seat | Governing Council | Executive Board negotiates; Secretariat executes | N/A | Legal due diligence; compliance canon | Publish summary MoUs and seat designation resolutions |

**Approvals, Recusals, and Escalations**

Approvals shall follow documented workflows and internal controls appropriate to IPSAS-compliant entities, with segregation of duties, traceable authorizations, and audit trails. Any matter exceeding delegated thresholds, or raising unresolved integrity or cyber risk concerns, shall be escalated to the Executive Board or Governing Council, as appropriate. Recusals are recorded in minutes and reflected in OCDS/IATI disclosures to the extent relevant to the contracting or activity record and consistent with lawful data-protection obligations.

**Independent Assurance and Public Accountability**

Delegated decisions are subject to independent audits and assurance engagements. Financial audits test IPSAS compliance and budget-to-actual presentation; procurement reviews test OCDS publication integrity and value-for-money; disclosure reviews confirm IATI completeness and timeliness; cybersecurity assessments examine ISMS effectiveness and Zero-Trust implementation maturity. Summaries of assurance reports and management responses shall be published, safeguarding legitimately classified information.

**References**


- **African Union — Digital Transformation Strategy (2020–2030).** AU DTS — official documents page. [au.int]

- **African Development Bank — High 5 Priorities.** AfDB “High 5s” overview. [afdb.org]
- **COMESA & World Bank — IDEA Programme.** World Bank Aide-Mémoire for IDEA with COMESA PCU; COMESA TOR for least-cost digital infrastructure planning. [documents1...ldbank.org], [comesa.int]
- **Open Contracting Data Standard.** OCDS — latest documentation. [standard.o...acting.org]
- **IATI — International Aid Transparency Initiative.** IATI Standard and governance. [iatistandard.org]
- **IPSAS — Financial Reporting in the Public Sector.** IPSASB official portal; 2024 IPSASB Handbook; Updated IPSAS 33 notice. [ipsasb.org], [ipsasb.org], [iasplus.com]
- **ISO/IEC 27001 — Information Security Management Systems.** ISO/IEC 27001:2022 overview. [iso.org]
- **NIST Zero Trust.** NIST SP 800-207 (final); NIST SP 1800-35 — Implementing a Zero Trust Architecture.

## Chapter Five — Financial Provisions and Fund Interface

**Financial Architecture and Governing Principles**

PCDE’s financial architecture is constituted to ensure lawful custody of programme resources, IPSAS-compliant accrual accounting, transparent procurement and contracting, and multi-window interface with development finance partners and private capital. The Executive Board shall approve annual budgets and operating plans; the Secretariat shall maintain general ledgers, asset registers, and cash-flow statements on an accrual basis in accordance with the IPSASB Handbook and applicable pronouncements, including IPSAS 24 for presentation of budget information in the financial statements.

Budget execution, commitments, obligations, and disbursements shall be recorded and disclosed through public dashboards and open datasets that map financial flows to activities, outputs, and outcomes, using the International Aid Transparency Initiative (IATI) Standard to facilitate donor interoperability and external scrutiny. Procurement and contracting processes shall be conducted and published under the Open Contracting Data Standard (OCDS), with machine-readable releases covering planning, tender, award, contract, and implementation stages to enable auditability and value-for-money analysis.

**Fund Interface with Sovereign and Non-Sovereign Windows**

PCDE shall structure financing in alignment with multilateral development bank practice for sovereign and non-sovereign operations. Sovereign windows may provide concessional grants and loans to eligible public entities and projects, while non-sovereign windows may finance commercially viable operations without sovereign guarantees, including eligible public enterprises and private entities, through instruments such as loans, guarantees, lines of credit, equity, and blended finance. This interface is intended to be interoperable with AfDB’s window architecture (ADB, ADF, and NTF) and its NSO policy framework, enabling crowd-in of private capital alongside public sector reforms and infrastructure investments.

**Instrument Catalogue and Accountability Chain (indicative)**

| Instrument | Window | Purpose and Typical Use | Accountability Chain |
|---|---|---|---|
| Concessional grant/loan | Sovereign (e.g., ADF/NTF) | Public infrastructure, policy reform support, national DEIC deployment | IPSAS accrual reporting; OCDS procurement; IATI activity and results disclosure. |
| Non-sovereign loan/equity | NSO (e.g., ADB private window) | SPVs for corridors, IXPs, data centres; commercially viable DEIC services | Financial covenants; IPSAS-based portfolio reporting; public OCDS/IATI releases as applicable. |
| Guarantees/blended finance | NSO/SO blended | Risk mitigation; PPP viability gap financing | Disclosure of guarantee terms; MEL-linked triggers; OCDS contract amendments and IATI updates. |

**Treasury, Banking, and Custody Controls**

The Secretariat shall maintain bank accounts with dual controls, segregate duties for initiation, approval, and reconciliation, and operate a Treasury Policy covering cash management, investment of surpluses, foreign-exchange risk, and interest-rate exposures. Financial statements shall be audited annually against IPSAS requirements, and budget-to-actual variances presented in accordance with IPSAS 24, with audit opinions and management letters disclosed subject to lawful confidentiality.

Disbursements under sovereign or non-sovereign financing shall be conditional upon satisfaction of covenants, safeguards, and procurement milestones evidenced through OCDS releases and verified under MEL protocols; forward plans and expenditure shall be reflected in IATI datasets to maintain continuous transparency of fund utilisation.

**PPP Structuring and Special Purpose Vehicles**

Where PCDE establishes or participates in special purpose vehicles (SPVs) for corridor assets or DEIC operations, the Executive Board shall approve the capital structure, shareholder-agreement clauses, dividend policies, and ring-fencing of public-interest obligations. Financing through NSO windows and PPP frameworks shall adhere to AfDB operational guidelines applicable to non-sovereign guaranteed lending to public enterprises, ensuring appropriate risk allocation, covenant design, and compliance with Bank policies on procurement and environment.

**Cybersecurity and Data-Protection Financial Controls**

Given the digital and trust-service nature of PCDE, the Secretariat shall operate an Information Security Management System aligned to ISO/IEC 27001 and implement Zero-Trust architecture consistent with NIST SP 800-207 and practice guides, ensuring secure custody of financial systems, payment processes, and disclosure platforms. In African jurisdictions, PCDE shall recognise and, where applicable, reference the AU Malabo Convention framework for cybersecurity and personal data protection in its financial systems design, classification policies, and cross-border data handling arrangements.

**Development-Finance Interoperability and Regional Integration**

In Eastern and Southern Africa, fund interface decisions shall take into account COMESA's IDEA programme coordination to avoid duplication and leverage regional knowledge and planning platforms for least-cost connectivity and financing models. Such coordination does not derogate from PCDE's disclosure and compliance duties under IPSAS, OCDS, and IATI.

# Chapter Six — Compliance, Audit, and Integrity

**Compliance Canon and Scope**

PCDE's compliance canon comprises internationally recognised standards and frameworks for financial reporting, procurement transparency, development-finance disclosure, cybersecurity, and anti-corruption. At minimum, PCDE shall maintain accrual-basis IPSAS financial reporting; publish contracting and implementation data in OCDS; disclose activity and results datasets using IATI; operate an ISO/IEC 27001-aligned ISMS and NIST SP 800-207 Zero-Trust controls; and adopt an anti-bribery management system consistent with ISO 37001:2025.

**Audit Arrangements**

Annual external audits shall be conducted by independent auditors applying public-sector audit standards recognised under the INTOSAI Framework of Professional Pronouncements (IFPP), including ISSAI 100 Fundamental Principles and the INTOSAI financial auditing standards aligned with IAASB ISAs, as applicable to public-sector entities. The audit scope shall cover financial statements, internal controls over financial reporting, procurement integrity and OCDS publication completeness, IATI disclosure accuracy, and cybersecurity and data-protection controls within the ISMS and Zero-Trust architecture.

The Secretariat shall maintain an internal audit function reporting to the Executive Board's Audit & Risk Committee, with authority to review compliance with Treasury Policy, procurement regulations, disclosure obligations, and technology controls, and to test corrective-action plans. Summaries of audit findings and management responses shall be published, safeguarding legitimately classified information under the Malabo Convention and applicable host-state data-protection law.

**Integrity, Anti-Bribery, and AML/CFT**

PCDE shall implement and continually improve an anti-bribery management system conformant with ISO 37001:2025, including risk assessment, due diligence on business associates, financial and non-financial controls, training, and an investigations and disciplinary framework for suspected misconduct. Certificates or assurance over conformity may be sought where proportionate to risk.

To mitigate money-laundering, terrorist-financing, and proliferation-financing risks in fund flows and PPP structures, PCDE shall adopt policies aligned with the FATF Recommendations, including beneficial-ownership transparency, enhanced due diligence for higher-risk relationships, and suspicious-activity reporting protocols consistent with national law. The risk-based approach mandated by FATF shall inform counterpart and transaction screening policies across sovereign and non-sovereign operations.

**Data Protection, Cybersecurity, and Incident Response**

PCDE shall ensure that personal data processing within programme operations adheres to applicable law and, in African jurisdictions, is cognisant of the AU Malabo Convention's provisions for data-protection authorities, data-subject rights, and cross-border data transfers. Breach notification and incident response procedures shall be embedded in the ISMS and Zero-Trust architecture, with post-incident reviews and corrective-action tracking reported to the Executive Board.

**Whistleblowing and Grievance Mechanisms**

The Secretariat shall operate confidential channels for reporting suspected integrity violations, procurement irregularities, financial misstatements, cybersecurity incidents, or privacy breaches. Whistleblowers shall be protected from retaliation consistent with best-practice guidance under

ISO-family governance standards and applicable law; reports shall be triaged, investigated, and resolved, with outcomes reflected in integrity dashboards and annual compliance statements.

**Sanctions, Debarment, and Remediation**
Vendors, contractors, or partners found to have engaged in bribery, collusion, fraud, money-laundering, terrorist-financing, or material misrepresentation shall be subject to sanctions up to debarment, contract termination, restitution, and referral to competent authorities. Integrity findings shall be published in accordance with OCDS guidance, and IATI activity records shall be updated to reflect sanctions that materially affect implementation. Remediation plans may include enhanced controls, training, and third-party monitoring as conditions for reinstatement.

**Assurance over Technology and Disclosure Systems**
Given PCDE's reliance on digital systems for finance and disclosure, the Executive Board shall commission periodic independent assessments of the ISMS and Zero-Trust implementation against ISO/IEC 27001 requirements and NIST practice guides, with summaries disclosed to the public and detailed reports provided to the Governing Council for oversight.

## Chapter Seven — Safeguards, Data Protection, and Cybersecurity

**Purpose and Scope**
This Chapter establishes a unified safeguards, privacy, and cybersecurity regime that binds all PCDE organs, project entities, suppliers, and delivery partners across sovereign and non-sovereign operations, ensuring that environmental and social performance, lawful processing of personal data, and protection of information assets are maintained to internationally recognized standards and to applicable regional and national legal orders. This regime is structured to interoperate with the African Development Bank's updated Integrated Safeguards System (ISS), the World Bank Environmental and Social Framework (ESF), the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), and relevant data-protection statutes, while integrating management-system standards for information security and privacy and Zero-Trust controls for hybrid environments.

**Environmental and Social Safeguards**
All PCDE-supported activities shall comply, at minimum, with borrower obligations equivalent in rigor to AfDB's ISS Operational Safeguards, including assessment and management of E&S risks and impacts; labour and working conditions; resource efficiency and pollution prevention; community health, safety and security; land acquisition and involuntary resettlement; biodiversity and natural resources; vulnerable groups; cultural heritage; financial intermediaries; and stakeholder engagement and disclosure. Where co-financed with the World Bank or aligned institutions, the ESF's ten Environmental and Social Standards and associated guidance notes shall be used to ensure harmonised risk classification, proportional mitigation, and grievance mechanisms across the project life cycle. The Secretariat shall maintain procedures for E&S screening, instruments (ESIAs, ESMPs, RAPs, SEPs), and periodic reporting consistent with these frameworks, and will disclose such instruments according to Chapter Eight.

**Data Protection and Cross-Border Data Governance**
PCDE shall implement a Privacy Information Management System that is conformant with ISO/IEC 27701:2025, assigning responsibilities for PII controllers and processors, codifying privacy risk assessment and treatment, and mapping controls to recognized privacy frameworks and applicable law. In African jurisdictions, processing of personal data shall be interpreted in light of the Malabo Convention's requirements for lawful processing, supervisory authority oversight, data-subject rights,

and cross-border transfers, without prejudice to stricter national legislation. In the European Union, or where EU residents' data are processed, the GDPR's principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability shall apply, including the obligation to notify personal-data breaches to the competent authority within the prescribed period.

Privacy by design and by default shall be practiced in all systems and services; data-protection impact assessments are mandatory for high-risk processing; data-subject rights (access, rectification, erasure, restriction, portability, objection) shall be facilitated through accessible mechanisms; and processor agreements shall include explicit instructions, security obligations, sub-processing restrictions, and audit rights. The Secretariat shall maintain a register of processing activities and a cross-border transfer log that records transfer mechanism and recipient safeguards, taking into account regional interoperability initiatives and guidance on privacy-framework interoperability.

**Cybersecurity Governance and Zero-Trust Architecture**

PCDE shall maintain an Information Security Management System aligned to ISO/IEC 27001, covering policy, roles, risk assessment, control implementation, monitoring, internal audit, and continual improvement, and shall implement a Zero-Trust Architecture in accordance with NIST SP 800-207 and practical deployment guidance to support identity-, device-, and workload-centric access decisions across on-premises and multi-cloud environments. Security and privacy controls shall be selected and tailored with reference to NIST SP 800-53 Revision 5, including access control, configuration management, identification and authentication, audit and accountability, system and communications protection, and privacy controls for PII. The Secretariat shall maintain documented secure-development practices, vulnerability and patch management, encryption at rest and in transit, key-management procedures, backup/restore testing, and supplier-security assurance, with periodic assessment of control effectiveness using NIST SP 800-53A procedures.

**Incident Response, Breach Notification, and Resilience**

A unified incident response plan shall define classification, escalation, containment, eradication, recovery, evidence preservation, and post-incident review, and shall incorporate notification triggers for privacy breaches and security incidents in accordance with applicable legal frameworks, including GDPR and Malabo Convention obligations where relevant. The Executive Board shall receive quarterly cyber-posture reports and, where material incidents occur, immediate briefings with recommended corrective actions; public summaries shall be disclosed under Chapter Eight, subject to lawful confidentiality.

**Regional Market and Payments Interoperability**

When operating in the COMESA region, PCDE shall align its safeguards for data and cybersecurity with regional digital-market facilitation initiatives, including EU-supported Safe Digital Boost Africa (SDBA) efforts to harmonise legal and technical standards for e-commerce and interoperable e-payments, ensuring complementarity with PCDE's privacy and Zero-Trust controls.

**Compliance Cross-walk (normative reference table)**

| Compliance Domain | Obligation | Reference |
|---|---|---|
| Environmental & Social | Apply AfDB ISS Operational Safeguards (OS1–OS10) or equivalent; disclose ES instruments | [consultati...s.afdb.org] |

| Compliance Domain | Obligation | Reference |
|---|---|---|
| Co-financing alignment | Apply World Bank ESF ESS1–ESS10 where applicable | [worldbank.org] |
| Information Security | Maintain ISMS certified/aligned to ISO/IEC 27001 | [standard.o...acting.org] |
| Zero-Trust | Implement ZTA per NIST SP 800-207 and practice guide | [fatf-gafi.org], [eufatf.com] |
| Security/Privacy Controls | Select/tailor controls per NIST SP 800-53 Rev. 5 and assess via SP 800-53A | [nvlpubs.nist.gov], [csrc.nist.gov] |
| Privacy Management | Operate PIMS conformant with ISO/IEC 27701:2025 | [iso.org] |
| Africa data law baseline | Observe Malabo Convention provisions | [iatistandard.org] |
| EU data law baseline | Apply GDPR where applicable | [eur-lex.europa.eu] |
| Interoperability guidance | Consider OECD privacy-interoperability toolkit for cross-framework operations | [goingdigit...l.oecd.org] |

# Chapter Eight — Transparency and Disclosure

**Purpose and Disclosure Philosophy**

Transparency is a constitutive feature of PCDE's fiduciary and governance architecture. Proactive disclosure enables external verification of value-for-money, deters misconduct, and supports public confidence and co-financing by sovereign and non-sovereign partners. PCDE therefore commits to machine-readable public disclosure of procurement and contract data under the Open Contracting Data Standard (OCDS), and to publication of activity, financial, and results data under the International Aid Transparency Initiative (IATI) Standard, subject only to narrowly tailored and lawful confidentiality restrictions.

**Open Contracting and Procurement Records**

All stages of the contracting process—planning, tender, award, contract, and implementation—shall be published in OCDS format with persistent identifiers, enabling end-to-end traceability of budgets, milestones, payments, amendments, delivery, and performance guarantees. The Secretariat shall maintain data quality controls and integrity checks, leveraging OCDS guidance and tooling for validation and codelist compliance, and shall link sanctions or integrity actions to the relevant OCDS releases and records.

**Development-Finance and Results Disclosure**

PCDE shall publish an authoritative IATI "organisation" file and timely "activity" files covering forward budgets, transactions, locations, results indicators, and linking to project documentation, with updates aligned to reporting cycles and co-financier requirements. Public dashboards shall visualise key outcomes (access, adoption, governance, market activation) and map to Agenda 2074 and MDB priorities; underlying datasets shall mirror IATI structures to facilitate reuse and independent analysis.

**Safeguards, Privacy, and Cybersecurity Disclosures**
Environmental and social instruments (e.g., ESIA, ESMP, RAP, SEP) and periodic safeguard reports shall be disclosed in accordance with ISS and ESF requirements, with redactions only where necessary to protect legitimate confidentiality (e.g., personal data, security-sensitive information). Privacy notices describing purposes, legal bases, data-subject rights, categories of recipients, retention periods, and cross-border transfers shall be published for all relevant services, aligned to the PIMS and applicable frameworks (Malabo Convention and GDPR as context-dependent). Cybersecurity policies, Zero-Trust principles, and annual posture summaries shall be made public, while the detailed ISMS artefacts and vulnerability information remain controlled in accordance with ISO/IEC 27001 and NIST guidance.

**Beneficial Ownership, AML/CFT, and Integrity Reporting**
To strengthen procurement integrity and financial probity, PCDE shall disclose beneficial-ownership information of awarded suppliers where legally permissible and shall publish summary AML/CFT controls and risk statements in alignment with the FATF Recommendations. Integrity incidents, sanctions, and debarments shall be linked to the affected OCDS records and reflected in IATI activity updates, preserving due-process confidentiality until decisions are final.

**Proactive Publication Schedule and Exceptions**
A publication schedule shall specify (a) procurement data release at the time of notice and at key milestones; (b) quarterly IATI updates for financials and results; (c) semi-annual safeguards portfolio reports; and (d) annual ISMS/ZTA posture summaries. Exceptions are limited to information whose disclosure would violate law, jeopardise safety or security, or infringe legitimate privacy interests; where redactions are applied, PCDE shall publish the legal basis and scope of redaction to the extent feasible.

**Regional Digital-Market and Payments Transparency**
In the COMESA region, where PCDE operations complement regional initiatives to enable interoperable cross-border e-payments and e-commerce under SDBA, PCDE shall disclose relevant standards-alignment statements and interoperability testing reports to support regulatory convergence and public trust in digital trade.

**Data Formats, Licensing, and Validation**
All disclosed datasets shall be openly licensed and provided in machine-readable formats consistent with the relevant standards' schemas and validation rules (OCDS JSON release/record packages; IATI XML/JSON), with versioning and clear provenance metadata. The Secretariat shall operate automated validators prior to publication, correct schema or codelist errors, and maintain a changelog for material corrections

## Chapter Nine — Amendments, Suspension, and Termination

**Purpose and Controlling Principles**
This Chapter governs the lawful modification of the Charter & Operating Manual, the temporary suspension of its application in whole or in part, and the orderly termination of the instrument or of specific PCDE operations. All actions taken under this Chapter shall preserve fiduciary probity, maintain

continuity of safeguards and disclosure, and protect data and information assets under the applicable privacy and cybersecurity regimes. In particular, survival clauses in respect of IPSAS-based financial reporting, open contracting disclosures, development-finance transparency, anti-bribery controls, AML/CFT measures, and information-security and privacy protections shall continue to bind the relevant parties for the periods specified herein and by applicable law and standards.

**Amendments**

The Governing Council may amend this Charter through a formal resolution following due notice and a recorded vote. A qualified majority shall be required for changes that materially affect: the legal personality and seat; decision rights and delegations; financial provisions and fund interface; and the compliance canon comprising IPSAS, OCDS, IATI, ISO/IEC 27001, NIST SP 800-207, ISO 37001, and the privacy baseline. All other amendments may be adopted by simple majority, provided quorum is met in accordance with Council Standing Orders. Amendments shall be published forthwith on the public registry and reflected in the controlled electronic version of the Charter, together with a summary of changes.

Prior to adoption of amendments that materially alter safeguards, disclosure, or data-protection obligations, the Secretariat shall circulate a legal and compliance impact memorandum setting out interoperability with the AfDB Integrated Safeguards System (ISS), the World Bank Environmental and Social Framework (ESF), and applicable privacy laws (including the AU Malabo Convention and, where applicable, GDPR). The memorandum shall be annexed to the Council resolution and published.

**Suspension**

The Governing Council may suspend the application of this Charter, or of specified provisions, in the following circumstances: a material and continuing breach by a PCDE Entity of core fiduciary, integrity, privacy, or cybersecurity obligations; force majeure events preventing lawful or safe operation; legally binding sanctions affecting performance; or the existence of a credible and immediate threat to the integrity or confidentiality of information systems or personal data. Where the precipitating cause concerns information-security or privacy, the Council shall rely on evidence from the ISMS and Zero-Trust controls and the incident-response record maintained by the Secretariat.

Except where immediate suspension is required to prevent irreparable harm, the Executive Board shall first issue a cure notice with a defined remediation plan and timetable, indicating any interim mitigations (including heightened disclosure, enhanced monitoring, or restricted disbursements). During suspension, obligations to maintain IPSAS accrual reporting, to publish contracting and financing data under OCDS and IATI, to operate anti-bribery and AML/CFT controls, and to protect personal data and information assets shall continue without derogation.

**Termination**

Termination may occur upon: expiry of the programme horizon if not extended; an explicit Council resolution to terminate the Charter following an independent review; illegality supervening across the programme's core jurisdictions; or the completion of all obligations and the closing of all financing and contractual instruments. Termination shall not discharge accrued rights or obligations, nor affect the validity of contracts and financing agreements already entered into; such instruments shall be wound down, novated, or assigned in accordance with their terms and with applicable law. A termination plan shall be approved by the Executive Board and endorsed by the Council, covering asset disposition, staff matters, outstanding audits, data retention and deletion, public disclosure, and stakeholder communications.

**Survival of Obligations (normative table)**

| Obligation Family | Minimum Survival After Termination or Suspension | Authority and Reference |
|---|---|---|
| Financial reporting and records (accrual) | Until completion of final audit and statutory limitation periods | IPSASB Handbook; IPSAS 24 (budget-to-actual) [idev.afdb.org] |
| Procurement and contract disclosure | Through contract close-out and archival retention schedule | OCDS — publication & records guidance [iso.org] |
| Development-finance transparency | Through last financial transaction and results reporting cycle | IATI Standard (organisation/activity files) [issai.org] |
| Anti-bribery management | Per sanction cycles and legal limitation; investigations conclude notwithstanding termination | ISO 37001:2025 [afdb.org] |
| AML/CFT measures and beneficial ownership | Per national law and FATF risk-based approach | FATF Recommendations (as amended Oct 2025) [africanres...rchers.org] |
| ISMS and incident records | Until completion of post-incident reviews and statutory retention | ISO/IEC 27001; NIST SP 800-207 (ZTA ops) [fatf-gafi.org], [d4dhub.eu] |
| Personal data protection | For the duration of lawful retention and deletion/erasure thereafter | GDPR; AU Malabo Convention; ISO/IEC 27701:2025 [comesacomp...tition.org], [standard.o...acting.org], [aftld.org] |
| Environmental & social safeguards | Through completion of ES commitments and grievance-mechanism closure | AfDB ISS; World Bank ESF [en.wikipedia.org], [unhcr.org] |

**Effect on Subordinate Instruments**

In the event of amendment, suspension, or termination, Regulations, Directives, Standard Operating Procedures, Host Country Agreements, and financing or PPP instruments shall be construed to the extent possible to remain effective and to give business efficacy to the Charter's intent. Where conflict is unavoidable, the Council's resolution shall specify the hierarchy and transition steps, subject to mandatory provisions of applicable law and co-financier covenants. All notices and public statements associated with actions under this Chapter shall be published pursuant to the disclosure regime in Chapter Eight.

## Chapter Ten — Final Clauses and Entry into Force

**Authentic Version, Language, and Interpretation**

This Charter is maintained in an authentic English version adopted by the Governing Council. Translations may be issued for operational convenience; in case of divergence, the authentic version

prevails. Questions of interpretation shall be resolved by the Governing Council upon reasoned advice from the Executive Board and the Secretariat's Legal Affairs unit, with due regard to the compliance canon and to applicable international and national instruments referenced herein, including the AfDB ISS, the World Bank ESF, ISO/IEC 27001, NIST SP 800-207, ISO 37001, ISO/IEC 27701, GDPR, and the AU Malabo Convention.

**Hierarchy of Instruments**
The hierarchy of PCDE instruments is as follows: this Charter & Operating Manual; Council Regulations and Council Resolutions of general application; Executive Board Regulations and Directives; Standard Operating Procedures adopted by the Secretariat; and project-specific instruments and contracts. In the event of conflict, the higher-order instrument prevails, subject to mandatory provisions of host-state law, treaty obligations contained in Host Country Agreements, and binding covenants of sovereign and non-sovereign financiers. The compliance canon and disclosure obligations shall be deemed incorporated by reference into subordinate instruments unless expressly and lawfully excluded.

**Severability and Non-Waiver**
If any provision of the Charter is held invalid or unenforceable by a competent authority, such invalidity shall not affect the remaining provisions, which shall continue in full force and effect, and the Council shall adopt such conforming amendments as may be required. Failure or delay in exercising any right under this Charter shall not constitute a waiver of that right. These clauses operate without prejudice to survival obligations identified in Chapter Nine.

**Notices and Depositary**
The Secretariat shall act as depositary of the authentic text, all amendments, and associated legislative history, and shall maintain the public registry and disclosures in accordance with the open-data commitments under OCDS and IATI. Formal notices under this Charter shall be issued by the Secretariat and recorded on the public registry together with date and time of issuance.

**Governing Law and Forum**
As an internal constitutive instrument, the Charter shall be interpreted in accordance with its text, purpose, and compliance canon. Disputes arising under project contracts, Host Country Agreements, or financing instruments shall be resolved in accordance with the governing law and dispute-resolution provisions contained in those instruments and the applicable host-state legal order, without prejudice to the environmental and social grievance mechanisms under the AfDB ISS or the World Bank ESF where co-financed.

**Entry into Force and Accession**
This Charter enters into force on the date of adoption by the Governing Council and remains effective through the programme horizon unless extended or terminated in accordance with Chapter Nine. PCDE Entities duly constituted thereafter are ipso jure bound by the Charter and by Regulations and Directives in force as of their constitution date. Regional bodies, host states, or partner institutions may accede to operational arrangements through Host Country Agreements or memoranda that reference and incorporate this Charter's compliance canon and disclosure regime.

**Force Majeure and Unforeseen Circumstances**
No party shall be liable for failure to perform obligations directly caused by events reasonably beyond its control, provided that such party promptly notifies the Secretariat, implements reasonable mitigations, and resumes performance as soon as practicable. Where force majeure materially affects

data protection or information-security obligations, mitigation shall include activation of incident-response and continuity plans consistent with ISO/IEC 27001 and NIST SP 800-207.

**Entire Instrument**

This Charter & Operating Manual, together with duly adopted Regulations, Directives, and referenced standards and frameworks, constitutes the entire constitutive instrument of PCDE and supersedes any prior conflicting provisions, without prejudice to the validity of acts lawfully performed under earlier instruments.

## Chapter Eleven — Closing Provisions and Strategic Outlook

**Purpose and Continuity**

This Chapter affirms the enduring nature of the PCDE Charter as a constitutive instrument for governance, compliance, and fiduciary architecture across the programme horizon. It is adopted as a binding framework for lawful, transparent, and equitable digitalisation, ensuring interoperability with international standards and regional development priorities without derogation from mandatory provisions of applicable law.

**Strategic Outlook**

The Governing Council shall maintain the Charter as a living instrument, subject to quinquennial strategic reviews to incorporate emerging standards, regulatory developments, and interoperability requirements with multilateral development banks, regional economic communities, and host-state legal orders. The programme's success depends on sustained collaboration among governments, private investors, civil society, and technology partners, underpinned by the compliance canon and disclosure obligations enshrined herein.

**Closing Declaration**

By adopting this Charter, all parties affirm their commitment to fiduciary probity, transparency, and technological resilience as foundational principles of inclusive growth. The Charter shall operate as a normative reference for all PCDE Entities, Regulations, and operational instruments, ensuring continuity of safeguards, disclosure, and integrity obligations throughout the 2026–2074 horizon and beyond, subject to survival clauses specified in Chapter Nine.