Africa-wide Guidelines for Sustainable Data Centre Development and Management

Energy efficiency, environmental impact, digital security and data sovereignty

Principal policy document

Draft for validation | October 2026

Prepared for the Technology, Innovation, Connectivity, and Infrastructure Division (TICID) of the United Nations Economic Commission for Africa (UNECA).

The views expressed are those of the author and do not necessarily reflect those of ECA or its member States.

Contents

Executive summary 3

1 Purpose and application 4

2 Planning and project decisions 5

3 Energy efficiency and power resilience 7

4 Environmental impact and circularity 9

5 Digital security and operational resilience 11

6 Data sovereignty and regional interoperability 13

7 Rights and equitable development 15

8 Adoption and accountability 16

Annex: Terms used in these guidelines 17

Executive summary

Africa needs reliable and affordable computing for public services, productive enterprises, research, and innovation. Data-centre investment can expand access, strengthen regional services, and support investment in electricity and connectivity. Each project should be judged by the services it makes possible and by the demand it places on electricity, water, land, and public resources.

One industry estimate puts operational capacity in Africa at just over 500 MW, with about 890 MW in development.[1] If capacity reached 5 GW, a scenario rather than a forecast, annual electricity use would be in the order of 50 TWh. That demand would arise while Mission 300 seeks to connect 300 million Africans to electricity by 2030.[2]

These guidelines respond to resolution 2026/2 of the ECA Conference of Ministers. They address energy efficiency, environmental impact, digital security, and data sovereignty through a common approach to project appraisal, operation, and national oversight.[3]

The first decisions arise before land, electricity capacity or public support is committed. Authorities should assess the full planned site, including later phases and related infrastructure, and establish who is responsible for each condition. Those decisions should govern commissioning, operation, expansion, and closure. Environmental requirements should follow resource use and local effects; security requirements should follow the harm that a service failure could cause.

Common methods for measuring energy and water will make results comparable. Each country should then set performance limits supported by its law and evidence. In water-stressed catchments, the authorised allocation and essential community needs should guide cooling choices. If saving water raises electricity use, the energy condition should account for that increase. Operators should demonstrate both the renewable electricity they claim and the power available during an outage.

For public and critical services, authorities should establish who can lawfully access the data, who controls the keys, and whether the service can be restored or moved to another provider. Domestic and regional hosting should be assessed against those requirements and applicable law. Any public support should state its fiscal cost and require delivery of specified services, domestic capabilities, and environmental results.

The accompanying Technical Companion provides the technical rationale, international comparisons, and national implementation tools. Its Annex D contains proposed reference values for validation; these are not continental requirements.

---

[1] Nairametrics, reporting Fortren & Company. Africa's data centre capacity exceeds 500 MW with 890 MW in pipeline, 27 July 2026. Secondary industry estimate. The 5 GW scenario is explained in Technical Companion section 2.1. Source.

[2] African Development Bank. Mission 300 overview. Source.

[3] Economic Commission for Africa. Report E/ECA/CM/58/6, resolution 2026/2, adopted 3 April 2026, especially paragraphs 2–8. Source.

1 Purpose and application

1.1 Objective and mandate

The objective is dependable computing that supports African economic transformation and regional integration, with efficient resource use, environmental protection, secure services and effective control over data and digital infrastructure.

A register of operating and planned facilities, supported by electricity forecasts and annual returns, will help countries assess the energy requirements identified in resolution 2026/2. Decisions on finance and technical assistance should follow the resulting evidence of demand, network needs, and delivery capacity.

The approach supports Agenda 2063, AfCFTA digital integration, the AU Data Policy Framework, the African Energy Efficiency Strategy (AfEES), and relevant Smart Africa initiatives. These instruments have different legal and institutional status. National adoption should identify the obligations that already apply and the additional measures being proposed.[4]

1.2 Status and users

The guidelines are recommendations to member States. They take effect through national laws, regulations, permits, contracts, or procurement instruments. Existing law and applicable treaty obligations continue to apply. Throughout this document, “should” states a recommendation and “may” identifies an option. The “shall” clauses in Technical Companion Annex B are model legal text. References here to operator duties describe requirements that countries are recommended to adopt.

The users are relevant ministries, regulators, public purchasers, operators, and investors. A designated coordinator should organise applications and information while preserving each authority’s statutory powers.

A single project dossier should bring the four areas together so that authorities can consider the effect of a decision about power, cooling or hosting on the other requirements.

1.3 Scope and proportionality

The guidelines cover purpose-built campuses, colocation and cloud facilities, enterprise and public-sector data centres, and modular or edge facilities providing continuous computing, storage or network services. Commercial availability ratings and business models should not determine regulatory duties by themselves.

Environmental duties should follow capacity, resource use, and site effects. Security and continuity duties should follow service criticality and the consequences of failure. A small facility carrying an essential public service may therefore need enhanced security while submitting a simplified resource return.

[4] African Union and continental partners. Agenda 2063; AU Data Policy Framework (2022); African Energy Efficiency Strategy (AfEES); Smart Africa Cloud and Data Centers for Africa initiative. Source.

2 Planning and project decisions

2.1 Capacity and facility bands

IT capacity means the rated electrical capacity available to computing, storage and network equipment, excluding cooling and other supporting systems. Commissioned IT capacity includes available capacity in commissioned halls or modules, whether occupied or not. Average IT load is measured use over time. Facility import capacity includes supporting systems and should be reported separately.

For annual resource reporting, the proposed bands are E1 at 20 MW and above, E2 from 1 MW to below 20 MW, and E3 below 1 MW of commissioned IT capacity. These are indicative administrative bands for national consultation. For screening and approval, authorities should assess the full planned IT capacity of a site or connected campus, including later phases. Each commissioned phase should meet the conditions applicable to it.

Countries should publish the thresholds they adopt and the reasons for them. The following values are starting points for consultation. Material local risk can require review below any capacity threshold.

Decision	Indicative starting point	Basis for national adjustment
Registration	National minimum, for example 100 kW	Visibility of material loads and the cost of keeping a register
Early site screening	1 MW of planned IT capacity	Effects on land, power, water, and neighbouring users
Grid-impact study	5 MW, or a smaller load on a constrained network	Actual system constraints, clustering, and reinforcement needs
Full environmental and social assessment	National law and material site or cumulative risk	Water stress, habitats, communities, and associated infrastructure
Heat-reuse appraisal	5 MW, where a plausible nearby user exists	Usable temperature, distance, demand, and cost
Whole-life carbon appraisal	10 MW and major redevelopment	Material embodied emissions and appraisal cost
E1 assurance duties	20 MW of commissioned IT capacity	Scale, reporting risk and availability of competent assessors

2.2 Joint energy and digital planning

National plans should distinguish operating facilities, financed construction and announced projects. Utilities should record connection reservations separately and reconcile duplicate applications. Forecasts should use phased loads, credible customers, and demand scenarios; announced megawatts should not be treated as certain consumption.

Energy and digital authorities should identify where proposed computing loads could justify new generation or network investment. Plans should test the effect on electrification, industry and other customers, including national energy-access commitments and Mission 300. Public investment should follow a credible assessment of both demand and available supply.[5]

Site-readiness assessment should document firm electricity at peak, grid-contingency capacity, local outages and power quality, total costs including backup, clean-energy deliverability, and seasonal water or climate constraints. A without-project comparison should identify any delay to household, business or public-service electrification and any network costs passed to other users. Shared-access benefits should count only when financed and verified.

2.3 A coordinated approval process

At concept stage, a developer should submit one pre-application dossier to the coordinator. It should identify the site and land rights, planned phases, customers and service functions, expected electricity and water needs, supply arrangements, cooling approach, connectivity, and any critical services. Relevant authorities should return one consolidated list of studies and approvals before irreversible commitments are made.

Before construction approval, the competent authorities should establish that the site, grid connection, water allocation, environmental conditions, and critical-service arrangements are acceptable. A connection decision should identify reinforcement, costs, delivery dates, capacity reservations, and any conditions still to be satisfied. Land access or an investment incentive should not be presented as assurance that power or water will be available.

At commissioning, the operator should provide evidence of the required permits, calibrated meters, safe operation, access controls, and tested continuity arrangements. During operation, annual returns and material changes should inform supervision. Expansion should trigger review of changed loads and cumulative impacts. Closure or transfer should address customers, data, equipment, waste, site remediation and remaining financial responsibilities.

Authorities should publish decision stages, information requirements, responsible institutions and review or appeal routes. Any fees for grid-impact or other required studies should identify the scope, charging basis and party responsible for payment. A single-entry point should reduce repeated submissions while preserving the separate decisions required by law. The Technical Companion provides a readiness assessment (Annex A) and model provisions (Annex B).

[5] African Development Bank. Mission 300 overview. Source.

3 Energy efficiency and power resilience

EE1 Measure energy consistently

Member States should require separate records of facility and IT energy, grid supply, on-site generation, and generator fuel. Annual power usage effectiveness (PUE) is annual facility energy divided by annual IT-equipment energy. Operators should declare the measurement boundary and category under ISO/IEC 30134-2. Metering intervals should be set nationally at a resolution sufficient to assess peaks and outages. Absolute energy use and average IT load should accompany PUE so that changes in activity are visible.[6]

EE2 Record and improve operating performance

New projects should submit auditable design PUE estimates for their site, expected load and operating conditions. Permits should record those assumptions. Operators should compare measured performance with the approved design after the first full operating year and explain material departures. Existing facilities should establish baselines and costed improvement plans. Authorities should calibrate operating limits from comparable data, engineering assessment, and compliance costs, with published transition and review arrangements. Adopted limits should be stated in enforceable instruments, with the measurement period, transition and authorised adjustments defined. Section 8.3 sets out the compliance process.

EE3 Agree supply and connection responsibilities

Large projects should have staged connection agreements identifying capacity, network works, delivery dates, curtailment, restoration, charges and responsibility for delay or cancellation. Utilities and regulators should test network reinforcement, demand flexibility, storage, and generation against the actual constraint before imposing a firm-capacity obligation. Deposits and financial security should reflect foreseeable unrecovered costs and reduce as that exposure falls. Charges should protect other customers from costs properly attributable to the project. Countries should permit and regulate customer-financed lines, substations and shared upgrades, defining ownership, maintenance, and reimbursement by later users without double recovery. Power contracts and PPPs should allocate delivery, currency, demand, and termination risks; public guarantees should be capped, time-bound and disclosed.

EE4 Select cooling for local conditions

Cooling appraisals should compare electricity, water, reliability, maintenance and whole-life cost using site conditions and the expected workload. In water-stressed catchments, lawful absolute and seasonal water allocations should govern. Where conserving water requires additional electricity, authorities should permit a documented, reviewed adjustment to the energy-performance condition without relaxing the water allocation. The relevant national instrument should set the evidence, duration, and review of that adjustment. ES2 applies to the same decision.

[6] ISO/IEC. ISO/IEC 30134-2:2026, Information technology — Data centres key performance indicators — Part 2: Power usage effectiveness (PUE). Source.

Heat-reuse installation should follow demonstrated local demand and technical and commercial feasibility; the appraisal threshold does not itself require installation.

EE5 Procure clean electricity credibly

Countries should enable lawful power purchase agreements, wheeling, direct supply, and suitable mini-grid arrangements, with clear network, balancing, and standby rules. Renewable claims should identify their source, attributes, and matching period, avoiding double counting. Annual renewable matching, additional generation, and dependable supply during outages should be assessed separately. National renewable milestones should reflect deliverable supply and transparent treatment of justified exceptions. Annual renewable matching is not firm hourly supply. Appraisals should assess hourly load, deliverable generation, storage, and backup; additionality claims should verify new financed capacity, commissioning, actual delivery, and renewable-attribute ownership. Technical Companion Annex D sets out proposals for validation.

EE6 Reduce recurring diesel dependence

Operators should record generator electricity, fuel, hours and purpose, distinguishing routine supply, commissioning, testing, and exceptional emergencies. Recurring use to cover predictable supply shortages should count as routine dependence. A facility with material routine dependence should have a funded reduction plan based on measured use, feasible supply improvements, and tested continuity needs. The plan should specify milestones, costs, responsible parties and review dates, distinguishing operator actions from utility or network commitments. National triggers should reflect local supply conditions and use the definitions in the Annex to these guidelines. Exceeding a trigger requires review and planning, not interruption of essential services.

EE7 Demonstrate resilience and efficient computing

Supply plans should test prolonged outages, fuel and renewable variability, equipment maintenance, and geographic recovery. Storage and other backup should be sized against those conditions, with safety, maintenance and recovery costs included. No universal battery duration or fuel technology is prescribed. Operators and customers should also manage underused equipment, procurement, and workload efficiency within their respective control. Colocation providers should supply tenant metering and clear operating interfaces; they should not be held responsible for computing decisions controlled by tenants.

Climate and infrastructure conditions differ within every region. Hot-arid sites should give particular attention to scarce water and heat rejection; humid coastal sites to cooling demand, corrosion, flooding, and route concentration; highland sites to the feasibility of air economisation. Hydro, geothermal, solar and wind opportunities should be assessed against deliverability and seasonal variation. Technology choices should follow the site assessment. Proposed small modular reactor (SMR) projects should also satisfy national nuclear safety, waste, water, grid, and full-life cost requirements.

4 Environmental impact and circularity

ES1 Assess sites and cumulative effects early

Authorities should screen proposals before irreversible land commitments. Assessment should cover land rights, community use, biodiversity, water, flooding, heat, fire and associated roads, lines, substations, and treatment works. The depth of assessment should follow national law and material risk, including cumulative demand from other developments. Smaller facilities in sensitive locations can require detailed studies. Meaningful consultation should include groups affected by changes in land, water, and electricity access.

ES2 Allocate water at catchment level

Water authorities should set annual and seasonal limits from catchment evidence, accounting for community supply, ecological needs, other users, and drought. Where local data support it, countries can add a WUE ceiling to those limits. New facilities in highly stressed catchments should normally avoid evaporative cooling with freshwater. An exception should state its reasons, comply with water law, and protect essential supply and ecosystems. Existing facilities need funded transition arrangements. The water allocation takes priority over a PUE target; EE4 explains how to record an energy adjustment. Water appraisals should also assess the opportunity costs of dry-season use relative to drinking water, agriculture, businesses, and ecological flows, alongside treatment and distribution costs. Reclaimed water, other non-potable sources, and drought-response arrangements should be evaluated without assuming that every litre requested has an alternative productive use.

ES3 Measure water and prepare for drought

Operators should record how much water a facility withdraws, consumes, and discharges, where it comes from and when demand peaks. Where cooling uses water, WUE should be reported alongside annual and seasonal volumes using the site measure defined in the Annex. A low WUE or closed internal loop can still consume too much water for the catchment. Reclaimed water, groundwater, and desalination each require assessment of local effects. Drought plans should show how critical services will operate within the permit limits.[7]

ES4 Report emissions on defined boundaries

E1 and E2 operators should report Scope 1 and Scope 2 emissions using recognised methods, including location-based and market-based Scope 2 where applicable. E1 should screen relevant Scope 3 categories and phase in material disclosures; E2 should begin with materiality assessment. E3 should provide energy and fuel quantities through simplified returns. Operator and tenant

[7] ISO/IEC. ISO/IEC 30134-9:2022, Information technology — Data centres key performance indicators — Part 9: Water usage effectiveness (WUE). Source.

boundaries should be clear, renewable attributes reconciled with energy returns, and gross emissions reported separately from credits.[8]

ES5 Keep equipment in productive use

Procurement and refresh decisions should consider remaining support life, energy use, repairability, embodied impacts and security. Operators should maintain asset and custody records and assess refurbishment or reuse before disposal. Data sanitisation should be verified against information risk and the media concerned. Schools, small firms, and other recipients should receive usable, supported equipment with realistic operating costs. Refurbishment targets should follow evidence of suitable stock and recipients.

ES6 Provide lawful recovery routes

Operators should fund take-back or equivalent arrangements for batteries, electronic equipment, refrigerants, and cooling fluids. Waste handlers and downstream destinations should be documented. Cross-border movements should comply with national law and applicable Basel and Bamako obligations; an assertion that equipment is reusable should not bypass waste controls. Regional recovery services should be developed where national markets cannot sustain safe treatment.[9]

ES7 Fund closure and residual responsibilities

Projects should have closure or transfer plans covering customer migration, residual data, equipment, fuel, chemicals, contaminated land, and costs. Financial assurance should reflect the likely liabilities and national law. A transfer of ownership should identify the party responsible for outstanding obligations and should not extinguish them.

[8] GHG Protocol. Scope 2 Guidance; Corporate Value Chain (Scope 3) Accounting and Reporting Standard. Use the applicable adopted methods and identify their edition. Source.

[9] Basel Convention Secretariat. E-waste amendments overview, including changes effective 1 January 2025. National prohibitions and applicable Bamako obligations require separate checks. Source.

5 Digital security and operational resilience

DS1 Designate critical services by consequence

The competent authority should identify essential services and systemic shared providers under national law, considering concentration, substitutability, and the consequences of disruption. Enhanced controls should follow that designation at any facility size. Countries should map the AU Convention on Cyber Security and Personal Data Protection to their treaty participation and domestic law; the operational controls below are recommendations under these guidelines.[10]

DS2 Secure the site and facility controls

Operators should apply layered physical access, auditable entry, protected power and cooling controls, fire safety, and disaster procedures. Biometrics should be used only where lawful, necessary, and proportionate, with protection and retention rules for templates. Flood, extreme heat and other site risks should inform the location of critical equipment and emergency access. Security measures should be tested in operation.

DS3 Maintain accountable security management

Facilities should have documented security and continuity controls, accountable managers, and supplier assurance proportionate to risk. Critical services should receive independent assessment covering the relevant service and facility. Procurement and contracts should identify responsibilities for the building, cloud platform, tenant systems, and data. Certificates should be checked for scope and supported by operating evidence.

DS4 Apply risk-based cyber controls

Critical services and privileged administration should use least privilege, strong authentication, controlled supplier access, logging and effective separation of customer, management, and facility-control networks. Zero-trust principles should inform access decisions, supported by patching, secure configurations and protected backups. Operators should assess supply-chain authenticity, support life and exit arrangements. Requirements should specify the needed assurance rather than mandate a particular product.[11]

DS5 Test independent recovery

Critical services should have defined recovery time and data-loss objectives and demonstrate restoration after loss of a site or supplier. Assessments should identify shared power, ducts, carriers, landing stations, keys, and other common failure points. Several contracts do not establish independent routes. Where physical diversity is unavailable, the service owner should agree and

[10] African Union. African Union Convention on Cyber Security and Personal Data Protection, treaty text and country participation. Source.

[11] National Institute of Standards and Technology. SP 800-207, Zero Trust Architecture (2020). Source.

fund an alternative continuity arrangement. Exercises should test the responsibilities of operators, providers, and customers together.

DS6 Establish compatible incident reporting

Countries should define significant incidents by service disruption, compromise of sensitive information, systemic or cross-border effects and harm to affected people. The proposed harmonised sequence is an early warning within 24 hours of awareness, an initial assessment within 72 hours and a final report within 30 days. If the investigation remains open, an interim report should give a follow-up date. Existing earlier duties should prevail; personal-data breach duties should continue under the relevant law.

National instruments should specify when awareness is established, the information required at each stage and the responsibilities of operators, controllers, and processors. Initial reporting should not await complete forensic certainty. Technical Companion Annex B6 supplies model provisions, including confidential handling and coordination of submissions. These deadlines are proposals for national adoption, not existing continent-wide legal duties.

DS7 Share threats through lawful channels

National incident response teams and supervisory authorities should establish cross-border contact and disclosure arrangements. Sharing should use agreed formats, confidentiality rules, and data minimisation. Authorities should protect necessary commercial and security information while ensuring affected customers receive usable notice under applicable law. Any protected sharing arrangement should state its recipients and purpose and should not excuse unlawful surveillance or negligent security.

6 Data sovereignty and regional interoperability

SO1 Classify information and services

Public bodies and regulated sectors should map information sensitivity and service criticality to national law before selecting hosting. Public information, personal data, sensitive or confidential information, and sovereign-restricted information should receive appropriate handling rules. The Annex to these guidelines sets out a common vocabulary for national adaptation. Classification policies should be available for scrutiny while sensitive system inventories remain protected.

SO2 Justify location requirements

A location restriction should identify the protected interest, evidence of risk, systems covered, less restrictive safeguards considered and a review date. Countries should check applicable AfCFTA obligations and exceptions, including the Protocol on Digital Trade's scope, entry into force and application to the State concerned. Government procurement and State-information exclusions should be assessed on their terms.[12]

SO3 Establish effective legal and operational control

Hosting assessments should examine jurisdiction, foreign legal demands, privileged access, encryption keys, subcontractors, audit, recovery, and redress. Domestic location or ownership should not be accepted as sufficient evidence of control. Arrangements for sovereign-restricted information should be expressly approved under national law and tested during supplier withdrawal and domestic disruption. Key custody should preserve both accountable control and recoverability.

SO4 Make procurement and exit enforceable

Public cloud and hosting contracts should identify processing, storage, and administration locations; subcontractors; access and key arrangements; incident duties; recovery objectives; audit; migration; charges; and deletion verification. Critical services should demonstrate export and restoration in an alternative environment before production acceptance. Duties should reflect the service purchased and the functions controlled by each party. Technical Companion Annex B8 provides a model procurement schedule.

SO5 Enable lawful regional hosting

Countries should compare domestic, regional and hybrid arrangements for the same workloads, protection, continuity, and whole-life cost. A regional agreement should define applicable law, supervision, transfer and storage permissions, access, emergency operation, complaints, disputes, and exit. Mutual recognition or a data embassy should not be assumed to waive national requirements. Landlocked and small island developing States should be supported in assessing practical alternatives where market scale or route concentration limits resilience.

[12] African Union. Protocol to the AfCFTA Agreement on Digital Trade (2024), articles 3, 20, 22 and 47; applicability is State-specific. Source.

Where regional hosting relies on cross-border electricity, authorities should verify trading rights, transmission and substation capacity, wheeling charges, scheduling, settlement, curtailment, and local backup. Regional power-pool membership or a supply contract alone does not establish firm deliverability to the proposed data-centre site. Energy and digital authorities should align such arrangements with applicable cross-border data rules.

SO6 Protect competition and interconnection

Authorities should promote competitive connectivity, feasible local and regional peering, and transparent access to essential infrastructure. Publicly supported colocation facilities should provide carrier-neutral access unless a lawful, reasoned constraint applies. Competition oversight should consider concentration and switching barriers. Routing conditions should preserve service continuity when preferred local routes fail.

SO7 Build domestic capability and usable access

Public support and relevant procurement should carry measurable commitments on technical skills, supplier development, or affordable computing access, appropriate to the project. These should specify beneficiaries, funding, and evidence of delivery. Local joint ventures can support capability where commercially and legally justified; equity requirements should be appraised separately. Outcomes should measure actual responsibilities, domestic value added and usable services, including connectivity and support costs, rather than nominal capacity or nationality alone.

7 Rights and equitable development

Lawful access to data should have a clear legal basis, legitimate purpose, necessity and proportionality, independent oversight, and effective redress. Residency requirements should operate alongside these protections. Operators should disclose government access requests to the extent permitted by law and protect personal information in reporting and threat sharing.

Workforce measures should cover recruitment, funded training, safe employment, retention, pay, and progression into technical and management responsibilities. Countries should assess barriers affecting women, young people and persons with disabilities and consult groups whose access to land, water or electricity may change. Where a project anchors shared generation, a mini-grid or water treatment, the appraisal should explain how surrounding communities can benefit and who pays for access.

Economic-benefit assessments should distinguish temporary construction work, sustained skilled employment and local procurement from wider productivity gains dependent on cloud adoption, connectivity, and skills. Where public support is granted, agreements should verify jobs, accredited trainees, domestic supplier purchases, and actual new electricity access against stated baselines, together with the net fiscal cost of incentives and guarantees.

Before granting tax relief, concessional land, public finance or preferential access to scarce infrastructure, authorities should appraise the project’s additional public contribution against its public cost. The appraisal should test demand, affordability, service access, domestic capability, shared infrastructure, and the no-support alternative. The award should state its ceiling, duration, delivery milestones, and remedies. This additional economic test should be proportionate and should not become a separate approval requirement for ordinary private facilities seeking no public support.

8 Adoption and accountability

8.1 National responsibilities

Each country should assign responsibilities and fund implementation through its existing institutions. The following allocation illustrates the functions to be agreed; national legal mandates should determine the final arrangement.

Function	Responsible institutions
Policy, coordination, and register	Lead ministry and designated coordinator
Supply, connections, tariffs, and system planning	Electricity regulator, utilities, and system operator
Land, water and environmental conditions	Competent planning, water, and environmental authorities
Critical services, security, and incidents	Designated security authority and incident response team
Privacy, transfers, and storage permissions	Data-protection and relevant sector authorities
Competition, procurement, and public support	Competition, purchasing, finance, and investment authorities

8.2 Proportionate implementation

Countries with limited registers or inspection capacity should begin with legal mapping, registration, basic energy and water records, site safeguards, and critical-service designation. Emerging markets should strengthen metering, new-project studies, and tested returns. Established hubs should add stronger assurance, calibrated performance limits, and cumulative infrastructure planning. A country can be advanced in one area and require support in another. Technical Companion Annex A can guide that assessment.

National plans should cost staff, meters, reporting systems, inspections, assessors, legal drafting, training, and appeals. Seasonal measurement and calibration should proceed alongside applicable safeguards. New projects should provide auditable design performance from approval; incomplete national data should not create an indefinite exemption. Legacy transitions should identify funded actions, milestones, and a review date.

8.3 Reporting, assurance, and compliance

Annual returns should use common definitions and the proportionate fields in Technical Companion Annex C. Operators should identify estimates, exclusions, and corrections. E3 should use simplified resource reporting; critical-service duties should apply independently. Authorities

should check reports according to risk and require independent assurance for the largest facilities where competent provision is available, with a published phase-in plan where it is not. Large-site reviews should also verify incremental firm and clean supply, shared network works, and actual electricity-access benefits against pre-project baselines.

Competent authorities should verify commissioning evidence and conduct periodic site inspections under a published schedule based on risk. Significant incidents, material expansion, or evidence of non-compliance should trigger additional review. The coordinator should maintain the decisions in one compliance record. Where national law uses a compliance certificate, it should identify the issuing authority, site and services covered, conditions, evidence, validity, and review date. It should record the relevant statutory decisions and preserve each authority's powers.

Public reporting should cover comparable resource and public-support results. Security weaknesses, personal information, and sensitive operational records should be restricted. A verified breach of an adopted PUE, WUE or other permit condition should require corrective action within a specified period. Persistent or serious breaches, false reporting, and failure to implement required actions should attract proportionate sanctions under national law, with reasons and appeal rights. Authorities should apply any authorised energy adjustment for water conservation when assessing PUE compliance. Unlawful water abstraction or imminent harm should receive prompt protective action under the relevant law. Suspension affecting essential services should include continuity arrangements. Technical Companion Annex B9 provides a model provision.

8.4 Regional support and review

ECA and willing partners could help countries compare reporting data, draft national provisions, and train the authorities who will administer them. Where expertise is scarce, countries could share assessors and specialist services for security, incident response, and recovery. Any role for ECA, the AU Commission, AFREC or regional economic communities should be agreed within their mandates and budgets.

The facility registers and returns should inform energy-demand assessment and joint infrastructure planning. Verified project results should inform finance and viable business models. Periodic review should examine measured resource use, service continuity, public benefits, compliance cost, and national implementation. ECA can use agreed aggregate findings in the progress reporting requested by resolution 2026/2.

Annex: Terms used in these guidelines

Capacity terms are defined in section 2.1. The following terms are used in chapters 3 to 6. Technical Companion sections 2.3, 2.4, 3.2 and 3.3 explain their basis.

Term	Meaning in these guidelines
Annual power usage effectiveness (PUE)	Annual total facility energy divided by annual IT-equipment energy on the declared measurement boundary, measured under ISO/IEC 30134-2. It is calculated from annual totals, not by averaging monthly or interval ratios.
Water usage effectiveness (WUE), site measure	Annual site consumptive water use in litres divided by annual IT electricity in kWh, for the same period and facility boundary. Withdrawal, consumption, and discharge are reported separately; national methods should reconcile the measure with ISO/IEC 30134-9.
Routine diesel dependence	Recurring generation used as ordinary supply or to cover predictable shortages, including repeated expected outages.
Exceptional emergency operation	Generation that protects service during an unforeseen disruption. Commissioning and scheduled tests are recorded separately from both routine and emergency use.
Routine diesel share	Routine diesel-generated electricity as a share of total annual facility electricity, on a consistent supply boundary before storage and without counting battery discharge twice. Countries set the trigger for a reduction plan; Technical Companion Annex D3 gives a reference value.
Critical service	An essential service or systemic shared provider designated by the competent authority under national law, considering concentration, substitutability, and the consequences of disruption.
Significant incident	An incident meeting the national definition based on essential-service interruption, serious compromise of information or systems, systemic or cross-border effects and harm to affected people.

Term	Meaning in these guidelines
Awareness of an incident	The point at which an initial assessment gives the responsible operator reasonable grounds to conclude that a significant incident has occurred. Complete forensic certainty is not required.
Information classes	Sovereign-restricted information; sensitive or confidential information; general personal information; and public information cleared for release. Countries map these classes to their existing classification schemes.