



department of communications and digital technologies



SOUTH AFRICAN APPROACH TO DATA CENTRE SERVICE ACQUISITION

Date: 24 FEBRUARY 2026

A leader in enabling a connected and digitally transformed South Africa!

- There is an estimated 10,800 to 12,000+ operational data centers worldwide, with the United States hosting the largest share at over 40%.
- The USA leads with 4,165–5,427 facilities, followed by Germany, the UK, China, and Canada.
- There is an observable symbiotic relationship between data centers, technological advancement, and digital transformation
 - Data centers act as the foundation or "backbone" of the modern digital economy, while technological advancements (like AI and 5G) drive the need for faster, more efficient data centers, which in turn enable businesses to achieve digital transformation.
- It can therefore be argued that Data Centers create a reliable basis for:
 - Technology advancement, especially AI, biotechnology and software innovation
 - Driving and accelerating digital transformation
- South Africa leads the African continent in terms of data center investments, boasting significant investment by companies such as Teraco, Africa Data Centres, Vantage Data Centres, Equinix and hyperscalers such as google, Amazon and Huawei.
- Much debate has arisen in terms of government reliance on data centers provided by foreign companies, specifically on how this usage affects data security and sovereignty, especially with the laws of some jurisdictions prescribing access to data stored by their companies, for certain reasons, irrespective of location.
- The debates mentioned above have given effect to calls for own data centers and full control thereof, specifically at government levels.

WHAT IS A DATA CENTRE

- A data center is a centralized physical or virtual infrastructure facility that houses networked computers, storage systems, and computing hardware to securely collect, process, store, and distribute massive amounts of data, acting as the backbone for modern IT operations, applications, and cloud services.
- There are four types of Data Centers, namely:
 - Enterprise: privately owned or leased, dedicated facility that houses an organization's critical IT infrastructure, including servers, storage, and networking equipment. They collectively manage, store, and process digital data to support business operations, applications, and cloud services.
 - Colocation: shared, third-party facilities where businesses rent space (racks, cages, or rooms) to house their own servers and networking hardware. They offer secure, high-uptime environments with professional power, cooling, and internet connectivity, allowing companies to avoid building private data centers.
 - Cloud: large-scale, off-site, third-party managed facilities that rent out computing power, storage, and networking infrastructure via the internet, and
 - Edge: small, decentralized facilities located close to end-users, devices, or data sources. They drastically reduce latency, speed up data processing, and support real-time applications like 5G, IoT, and autonomous vehicles.

DATA CENTERS vs TRADITIONAL INFRASTRUCTURE (SERVERS)

CONTROL	OUTSOURCED TO A THIRD-PARTY PROVIDER (COLOCATION).	COMPLETE IN-HOUSE CONTROL OVER HARDWARE/DATA.
Scale/Capacity	Large facilities housing thousands of servers.	Small to medium, depending largely on office space.
Location	Dedicated, specialized building.	Office designated location
Control	Outsourced to a third-party provider (Colocation).	Complete in-house control over hardware/data
Cost Model	Pre-agreed monthly hosting fees (Operational expenditure)	Upfront investment for hardware and cooling systems (Capital expenditure)
Reliability	High reliability supported by multiple redundancy systems (power, network).	Lower, reliability and prone to outages if not properly maintained.
Cooling	Advanced (Liquid/Immersion cooling, raised floors).	Standard heating, ventilation & cooling systems
Security	Robust; multi-level, 24/7 security, cameras.	Security limited by what the organization can afford at a particular time.
Scalability	Rapid; flexible; easy to add resources	Limited by capital expenditure thresholds, with upgrades requiring longer time
Support	24/7 on-site technical support.	In-house IT staff required.
Sustainability	Higher due to optimized energy efficiency.	Harder to manage energy efficiency due to building structure.

BENEFITS OF GOVERNMENT DATA CENTER OWNERSHIP

- **Enhanced Security and Compliance**
 - The built and design meets strict, specialized security requirements (security & privacy by design) for protecting sensitive government data, implementing advanced firewalls, encryption, and access controls
- **Data Sovereignty and Control**
 - Infrastructure ownership reduces reliance on private, potentially foreign, third-party providers, ascertaining that data remains within local jurisdiction.
- **High Reliability and Reduced Downtime**
 - Government data centers focus primarily on high standards for continuity, robust backup systems, and ensuring reliable, uninterrupted service for critical public applications
- **Economic Impact and Job Creation**
 - Economic benefits in terms of construction jobs, long-term employment, and increased property tax revenue, which supports public services and enhance government service delivery
- **Cost Efficiency and Sustainability**
 - Allowing for centralized, shared facilities allow for all government departments would reduce operating costs compared to fragmented, individual agency, or departmental server rooms. Shared government data centers can also improve energy-efficiency and ensure integrated cooling systems
- **Improved Citizen Services:**
 - By centralizing data, agencies can streamline operations, leading to better digital services for the public.

The National Data and Cloud Policy provides for a shared facility under the custodianship of the State Information Technology Agency, to:

- Government data shall be stored in a unified, scalable and cloud-enabled data centers, supported by enabled data-sharing and interoperable systems, providing a single view of the citizen and supported by redundancies in other locations to support back-up and business continuity requirements.
- The State Information Technology Agency (SITA) shall be the responsible authority, by virtue of its legislative mandate, to source data infrastructure and cloud services for government, ensuring the development and monitoring of service level agreements that guarantee consistent, reliable and secure data and cloud services for government. In this regard, government should make sure that SITA is adequately capacitated and resourced to discharge its responsibilities
- Data centers in South Africa should meet the following compliance requirements:
 - Not to be built in restricted areas such as heritage sites, national key points or land designated for land reform.
 - Not located in areas prone to natural disasters or social disturbances.
 - Display or provide verifiable certification credentials to all potential customers.
 - Data centers used by government should comply with a fault tolerant design that would provide a minimum uptime of 99, 995%.).
 - Provide for energy self-generating capacity
 - Align with South African environmental provisions in terms of carbon emissions reduction.

POLICY PROVISIONS IN TERMS OF DATA CENTRES (Cont.)

- All digital technologies used by government should incorporate cybersecurity-by-Design (including warning systems to detect and inform clients of potential cybersecurity threats in their infrastructure) covering the entire lifecycle of data collection, processing, use, storage, mining and destruction
- Government data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa.

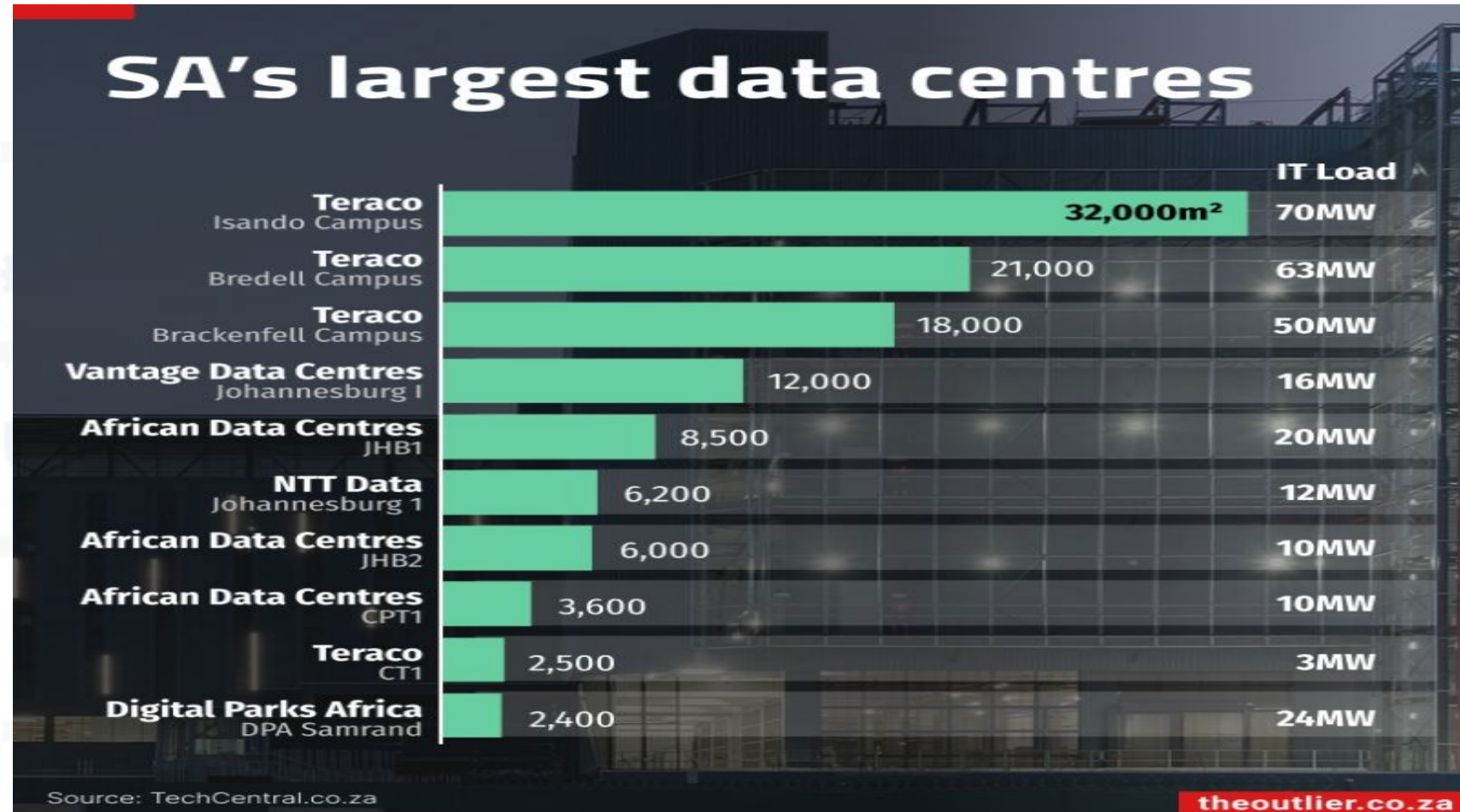
- **Gauteng (Primary Hub):** Johannesburg is the core hub for data center capacity, holding nearly half of Africa's active data center capacity and serving as the main landing point for landlocked neighboring countries. The key data center operators are:
 - Turaco (Digital Realty): Operates major campuses in Isando and Bredell.
 - Africa Data Centres (ADC): Significant facilities in Midrand and Samrand.
 - Vantage Data Centres: Operates a massive 80MW campus in Waterfall City.
 - Equinix: Established a data center (JN1) in Johannesburg.
 - Hyperscalers: Google (Africa region), Microsoft (South Africa North), and Huawei Cloud are heavily invested here.
- **Western Cape (Cape Town) - Secondary Hub.** The key data center operators are:
 - Teraco: Operates a major campus in Brackenfell.
 - Africa Data Centres (ADC): Operates facilities in Cape Town.
 - Hyperscalers: AWS has three Availability Zones in Cape Town, while Microsoft has its South Africa West region located here.
- **Special Economic Zones (SEZs) – Strategic Growth.** These are driven by cheaper land, reliable power potential, and tax incentives (e.g., 15% corporate tax rate).
 - Coega (Eastern Cape): Targeted for new data center developments.
 - Richards Bay (KwaZulu-Natal): Targeted for new data center development
- **SITA data Centers:** Operates two main data centers in Pretoria (Centurion & Beta) and 34 switches across the Northern Cape, Kwazulu-Natal, Eastern Cape, Western Cape and free State.

CAPACITY NEEDED FOR SOUTH AFRICA TO BE A GLOBAL PLAYER IN AI AND OTHER EMERGING TECHNOLOGIES

- The McKinsey study (Building data centers for Africa's unique market dynamics), South Africa will need to scale up its data center capacity from the current 350 MW toward a projected 1.5 to 2.2 Gigawatts (GW) by 2030 if it wishes to become a significant global player in Artificial Intelligence (AI) and emerging technologies.
- AI needs specialized data centers with high-density racks that need advanced liquid cooling requirements, unlike traditional data centers.
- In addition to cooling requirements, AI data centers have very high energy consumption, meaning that reliance on the national grid will not be feasible.
- South Africa is currently a scarce water resourced country. Although energy supply has been stabilized, more work is required to capacitate and sustain the resilience of the national grid.
- Private sector players such as Teraco have already indicated their intentions to build solar farms to augment their energy requirements.
- AI Data Centers are not just expensive and requiring monumental investment funding, they are also higher consumers of electricity and water.
- Government interventions in this instance would ideally focus on:
 - Encouraging investment in AI and emerging technology driven data centers
 - Establish partnerships with key data center investors to enable leveraging on their new infrastructure
 - Examine funding models that will make it feasible to upgrade or invest in new advanced data centers supporting AI and emerging technologies
 - Diversifying energy sources while strengthening the reliability of water supply
 - Strengthen SITA's capacity to operate and manage advanced data centers.



CURRENT CAPACITY OF SOUTH AFRICA'S LARGEST DATA CENTERS



DATA CENTRE IMPACT ON GOVERNMENT STRATEGIC PROGRAMMES

- Government's Digital Transformation Roadmap has as its mission to deliver world class services for all by developing and leveraging trusted digital technologies, infrastructure and capabilities across the whole of government's, with the primary focus being on:
 - Proactive, accessible human centered government services for people and businesses
 - Interoperable systems and data exchange for improved operations and data-driven decision-making
 - An interoperable digital identity ecosystem for transacting with government
 - An inclusive, secure, cashless digital payment system for society
 - Integrated government planning and linked systems providing on-stops services.
- Data centers can support and enhance government's service delivery and digital transformation initiatives through:
 - Improved efficiencies, by hosting of online portals creating accessible online services for payments, registrations, queries and even participation in government policy and legislative development.
 - Stronger reliability, ensured by availability standards (e.g., 99.995% uptime) and redundancy, critical in enabling government to respond to emergency services and ensuring that key public services (public health, education etc.) operate without interruptions.
 - Data-driven decision-making, driven by centralized data storage environments that enable interoperable systems and data exchanges supporting data analytic capabilities to proactively identify service delivery solutions (traffic, crime detection, infrastructure gaps)
 - Strengthened mitigation against cyber-attacks through encryption, firewalls, 24-hour security.
 - Supporting scalability, by ensuring that storage and processing resources are available based the extent of demand during different periods.

DATA SOVEREIGNTY AND SECURITY SAFEGUARDS

- The data center landscape is primarily dominated by North America (USA and Canada), followed by Europe (Germany and UK) and then China.
- The Digital future/destiny of developing countries will not only be impeded by limited access to technologies, but may also be controlled by those that dominate the technology sphere
 - Data sovereignty cannot be addressed separately to digital sovereignty.
- Although developing countries, including South Africa, are increasing their technology uptake, capacity aspects are not being addressed at the same pace:
 - Digital infrastructure capacity
 - Reliable energy supply
 - Research and Development capacity
 - Skills capacity
 - Regulatory capacity
- These constraints are recognized in various documents developed by government, including The Presidential Commission on 4th Industrial revolution Report, The National data and Cloud Policy, the National Infrastructure Plan 2050, The Digital Transformation Roadmap, among others.

- South Africa is largely ahead of its continental counterparts in addressing issues of data and digital sovereignty:
 - The development of data privacy and security protection policies and legislation, i.e. The Protection of Personal Information Act (POPIA), The Cybersecurity Policy Framework and The Cybercrimes Act
 - The establishment of the Information Regulator to oversee and monitor the implementation of POPIA
 - Significant progress in broadband infrastructure rollout
 - Significant progress in addressing the reliability of energy supply
 - Although South Africa has invested R43, 413 billion in research and development for the 2023/24 financial year, it still falls short of the 1.5% of the GDP as required to support economic expansion goals.
 - Digital skills interventions are happening at different levels though the demand for technology professionals keeps increasing (Pnet's Job Market Trends Report for November 2025).

- From a government data security and sovereignty perspective, SITA has ensured the following:
 - Operating two national data center facilities—Centurion (Primary) and Beta (Secondary)—forming the backbone of government digital infrastructure.
 - Hosting mission-critical systems and sensitive government data, accessed via 34 interconnected switching centers nationwide. The 34 switching centres are critical to SITA core network availability, enabling resilient connectivity to government departments.
 - The data center facilities are designed for high availability, resilience, and national-scale service delivery, ensuring continuous government operations.
 - Year-to-date uptime and availability performance comparable to leading market operators, reflecting mature and reliable operations.
 - The Data Center facility are classified as National Key Points and strategic national assets, subject to stringent physical security, access control, continuous monitoring, and governance oversight

DATA SOVEREIGNTY AND SECURITY SAFEGUARDS

- In the medium and long-term, government will need to strengthen interventions in the following areas to preserve its data sovereignty and security:
 - The establishment of a high-capacity national integrated government data center, with enabled data exchange and interoperable systems incorporating privacy and cybersecurity protection by design, with strong redundancy provisions and adhering to international uptime and other related security and privacy protection standards.
 - A repurposed and fully capacitated SITA, overseeing the Operation of the national data center and ensuring that all government data hosted within South Africa, continuing to ensure full compliance with POPIA, the Cybercrimes Act, and DCDT policies, supported by data classification and controlled access
 - The capacitation of the Information Regulator to sustain and strengthen its implementation of POPIA as well as related institutional mechanisms to give effect to that. Same capacitation should also be applied to the monitoring and implementation of the Cybercrimes Act.
 - Targeted digital skills interventions necessary to support technological development, adoption and utilization in South Africa, focusing on data analytics, software development, data center design and management, cloud technologies and other related skills to reduce dependents on other jurisdictions.
 - The finalization of cybersecurity legislation and establishing the relevant institutional mechanisms to strengthen South Africa's digital trust environment and encourage increased technology uptake and adoption among all citizens
 - Strengthen South Africa's participation on regional and international collaboration structures and mechanisms to circumvent cyberthreats and other data and technology-driven crimes.
- In the short-term, government will leverage on the capacity of industry to address its data storage requirements, while ensuring that data security and privacy requirements are addressed.

