GOVERNMENT NOTICE NO. 85 published on 27/3/2026

THE TANZANIA COMMUNICATIONS REGULATORY AUTHORITY ACT,
(CAP. 172)

RULES

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY (PUBLIC DATA CENTRES) RULES, 2026

PART I
PRELIMINARY PROVISIONS

PART II
OPERATIONAL REQUIREMENTS FOR LICENSEES

PART III
MANAGEMENT OF PUBLIC DATA CENTRES

PART IV
PUBLIC DATA CENTRE TECHNICAL REQUIREMENTS

PART V
PUBLIC DATA CENTRE DEPLOYMENT

PART VI
MAINTENANCE REQUIREMENTS

PART VII
GENERAL PROVISIONS

THE TANZANIA COMMUNICATIONS REGULATORY AUTHORITY ACT,
(CAP. 172)

RULES

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY (PUBLIC DATA CENTRES) RULES, 2026

PART I
PRELIMINARY PROVISIONS

Citation

1. These Rules may be cited as the Tanzania Communications Regulatory Authority (Public Data Centres) Rules, 2026.

Application

2. These Rules shall apply to network facility licensees who provide public data centre services.

Interpretation

3. In these Rules, unless the context otherwise requires-

Cap. 172 "Act" means the Tanzania Communications Regulatory Authority Act.

"Authority" means the Tanzania Communications Regulatory Authority established under the Tanzania Communications Regulatory Authority Act;

Cap. 172

"carrier neutral data centre" means a data centre facility that enables a licensee to provide network connectivity services to customers inside and outside the data centre without any discrimination between the licensees;

"co-location" means accommodation of two or more licensees, switches, antennas or other electronic communication equipment in, or on a single building, tower or other structure;

"data centre" means a facility dedicated to the centralised accommodation, interconnection and operation of

information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and cooling, environmental control together with the necessary levels of resilience and security required to provide the desired service availability;

"data centre customer" means a person who acquires services from a licensee;

"dedicated servers services" means a type of hosting service where an entire physical server is dedicated to a single client or organisation;

"licensee" means a holder of network facilities services licence issued by the Authority for the provision of public data centre services;

"N" means the minimum number of resources or components needed to operate a system;

"N+1" means the configuration that adds one extra component to the primary system, ensuring service continuity during a failure or maintenance for effective redundancy;

"private data centre" means a data centre operated by an entity whose sole purpose is the delivery and management of the service to its employees and customers;

"public cloud computing service provider" means any person who provides cloud computing services to the public through owned or via rented public data centres;

"public data centre" means a data centre that provides to the public services for co-location or co-hosting of a customer's network, servers and storage equipment;

"public data centre services" means the collection of all the supporting components necessary for the proper operation of a data centre which may include hardware, software, processes and personnel;

"rack" means a standardised frame for mounting electronic equipment, such as servers, network devices and storage units;

"2N" means the configuration that duplicates the entire system, providing a higher level of redundancy and reliability; and

"2N+1" means the configuration that has twice the amount of equipment needed for operation, plus an additional backup allowing for multiple simultaneous failures without service interruption;

PART II
OPERATIONAL REQUIREMENTS FOR LICENSEES

Licensing GN No. 57 of 2018

4. A person who intends to provide public data centre services shall-

(a) obtain a licence from the Authority in accordance with the Electronic and Postal Communications (Licensing) Regulations;
(b) comply with the minimum technical specifications specified by the Authority; and
(c) not commence the construction of a public data centre without obtaining the approval of the Authority.

Carrier neutral data centre

5. A licensee shall ensure that the data centre is carrier neutral and operates on an open access basis that includes fair, transparent interconnect and peering ecosystem across multiple carriers, internet service providers, content providers and internet exchanges, subject to applicable laws and regulations.

Services by licensee

6. A licensee may offer the following services:

(a) collocation services including appropriate space, power and cooling systems to data centre customers who can provide their servers and other communication equipment;
(b) lease of racks by allowing data centre customers to host servers and other communication equipment;
(c) dedicated servers to data centre customers;
(d) hosting of cloud service providers;
(e) provide equipment installation, maintenance, operations and associated accessories services to data centre customers within the data centre; and

(f) any other service related to the public data centre as may be determined by the Authority.

Provision of services to foreigners

7. The licensee may offer services to a foreign entity provided that such an entity is legally recognised in its country of origin.

PART III
MANAGEMENT OF PUBLIC DATA CENTRES

Managem ent of data centre

8. A licensee shall-

(a) at all times ensure that he holds a valid licence and all relevant certificates related to the service provided;

(b) submit to the Authority all design and related deployment documents;

(c) facilitate connectivity for data centre customers and ensure carrier neutrality and fair treatment of all customers without discrimination;

(d) transparently disclose fees, nature of the services provided and technical details of the data centre in advance to customers and interested parties;

(e) implement regular preventive maintenance to manage and maintain public data centres to ensure business continuity;

(f) provide timely and effective customer support, including assistance during setup and configuration;

(g) design and deploy public data centres in accordance with national and international standards for reliability and security;

(h) conduct periodic internal security audits to identify potential threats and vulnerabilities at the server, application and operational levels, ensuring continuing security and preventing unauthorised access;

(i) perform periodic assessments to evaluate the security level of the data centre building, identifying potential threats and weaknesses, and

taking necessary measures to address any defect or potential threat found in the security level;

(j) secure customer data by implementing measures to prevent data breaches and other security threats;

(k) maintain recordings and records for closed-circuit television and detection systems for a minimum of six months;

(l) ensure public data centres are scalable to accommodate future industry growth;

(m) inform the Authority immediately of any penetration, cyberattacks or security incident, working to assess damages and notify users or hosted individuals in coordination with the Authority;

(n) conduct training for employees on data centre services at least once a year;

(o) install a scalable centralised management and monitoring system tool capable of doing fault management, configuration management, security management, report generation, alerting, monitoring the critical servers and log monitoring of data centre;

(p) maintain a service level agreement with its customers in accordance with the laws of Tanzania;

(q) implement best practices to minimise the negative environmental impact of public data centres, including reducing unnecessary energy consumption and enhancing waste management practices;

(r) inform their customers on the insurance coverage they have against any liability for their customers to assess the exposure to risks and decide on their insurance coverage accordingly;

(s) unless otherwise agreed by the parties, assume responsibility to customers for any damage or loss resulting from any act or omission by the licensee or its agent, incurring liability under these Rules or any other law in force in Tanzania; and

(t) submit data centre performance reports to the Authority every quarter.

Personal data protection

9.-(1) The licensee shall-

(a) not make changes or assess clients' data without the consent of the data subject;

(b) implement technical measures to protect customers' content against theft, loss, tampering, or alteration.

(2) Notwithstanding subrule (1), in the implementation of these Rules, the licensee shall comply with the Personal Data Protection Act.

Shutdown of data centre

10.-(1) A licensee who intends to shut down a data centre shall, except in cases of natural disasters, give written notice to the Authority and customers at least one year before shutting down.

(2) Without prejudice to subrule (1), the Authority may allow shutdown of a data centre or services within a period shorter than that specified in subrule (1), if it is satisfied that the licensee has reached an agreement with its customers to cease the services.

Backhaul services

11. A licensee shall ensure that-

(a) a data centre customer requesting the service has the right to choose a licensee who will provide backhaul services; and

(b) the data transmission route has sufficient capacity to carry the volume of service required by the data centre customer, on the same terms and conditions as those offered to other data centre customers.

Information retention requirements

12.-(1) A licensee shall maintain accurate and up-to-date information about their data centre, including used and available space, cooling and power capacity, and other licensees providing services within the data centre.

(2) A licensee shall provide any information provided in subrule (1) when requested by the Authority.

(3) The Authority may appoint an independent auditor to conduct inspections, checks and controls on its behalf.

PART IV
PUBLIC DATA CENTRE TECHNICAL REQUIREMENTS

General technical requirements GN No. 21 of 2018

13. A licensee shall ensure a public data centre has-

(a) high availability as provided in the Electronic and Postal (Quality of Service) Regulations; and

(b) high redundancy allowing concurrently maintainable (N+1) or fully faulttolerant (2N or 2N+1) to ensure service continuity even during a failure or maintenance.

Design requirement

14. A licensee shall ensure the following in designing a public data centre:

(a) adequate power and cooling for servers and other equipment;

(b) the data centre is highly available and scalable with redundant components and multiple paths for data to flow;

(c) physical and electronic security measures are available to protect the data centre against unauthorised access and data breaches;

(d) provision of a structured cabling system to organize and manage cables, enhancing the overall appearance and functionality of the data centre;

(e) provision of systems for remote monitoring and management of the public data centre to assess the performance of its infrastructure;

(f) scalability and adaptability to changes in technology and data centre customers' requirements;

(g) incorporating green energy sources into the infrastructure; and

(h) compliance with the technical specifications specified under the minimum technical specifications for public data centres as provided by the applicable national and international standards.

PART V
PUBLIC DATA CENTRE DEPLOYMENT

Data centre planning

15. A licensee shall consider the following when planning the deployment of a public data centre:

(a) locating the centre in an area close to reliable sources of power and low risk from natural disasters including floods or earthquakes;
(b) ensuring a proper data centre layout, including the placement of servers, storage devices, and other equipment;
(c) providing adequate space between racks and pathways to allow for maintenance and accessibility;
(d) accommodating current and future requirements for co-location space, power, cooling, storage equipment, and other related infrastructure; and
(e) consider the number of employees and customers who will access the data centre, along with their specific needs.

Power systems

16. A licensee shall-

(a) ensure the presence of an uninterruptible power supply in the data centre in the event of a power outage to ensure continuous operational functionality;
(b) implement adequate power distribution units to distribute power to servers and other equipment in the data centre;
(c) deploy monitoring systems for the monitoring and control of power usage in the data centre;
(d) utilise standard power cables to connect data centre equipment to the power sources;
(e) install protection devices to safeguard the data centre from power surges and voltage spikes; and
(f) properly ground the data centre to ensure the safety of equipment and personnel working in the data centre.

Cooling systems

17. A licensee shall-

(a) ensure sufficient cooling for all equipment hosted in the public data centre in accordance with applicable international standards;

(b) implement a raised floor or suspended ceiling, or other configuration to provide more flexible cooling options;

(c) maintain temperature levels and humidity conditions within the public data centre as recommended by the manufacturers for the installed equipment; and

(d) arrange cabinets and racks in a configuration that manages airflow to conserve energy and reduce cooling costs.

Security systems

18. A licensee shall-
(a) implement physical security controls, including access controls, surveillance cameras, and perimeter fencing, to prevent unauthorised access to the public data centre;
(b) conduct regular security assessments to identify and mitigate security risks on time;
(c) establish a disaster recovery and business continuity plan along with a suitable data backup and recovery infrastructure to ensure data recovery in the event of a disaster or data loss;
(d) ensure that the public data centre architecture supports the appropriate data retention as directed by the Authority; and
(e) regularly conduct capacity building to employees on services provided by the public data centre.

Fire protection systems

19. A licensee shall-
(a) install early warning detectors including smoke or heat detectors that are connected to an alarm and monitoring panel;
(b) implement fire alarm systems to alert occupants of the public data centre about the presence of smoke, heat, or fire using audible or visual alarms; and
(c) provide fire suppression equipment including fire extinguishers and other related tools.

PART VI
MAINTENANCE REQUIREMENTS

Preventive maintenance

20. A licensee shall -
(a) continuously monitor the public data centre to detect faults and take appropriate actions; and
(b) conduct regular preventive maintenance without interfering with the normal operation of the public data centre.

Corrective maintenance

21. A licensee shall -

(a) adhere to the restoration time requirements specified in the Service Level Agreement (SLA) during corrective maintenance;

(b) conduct all repairs in compliance with national, international standards and regulatory requirements;

(c) perform tests to verify the accuracy of the repairs undertaken; and

(d) keep a record of all activities performed, including the date, restoration time, reasons for failure and actions taken to correct the faults.

Critical outages

22.-(1) A licensee shall handle a critical outage resulting from scheduled maintenance by -

(a) providing notice to customers at least 48 hours before carrying out the maintenance;

(b) notifying the Authority at least 72 hours before executing the scheduled maintenance; and

(c) issuing a notice regarding affected services, impact and expected restoration times.

(2) A licensee shall handle critical outages resulting from unplanned maintenance by -

(a) notifying the Authority and customers within one hour of the outage, specifying the affected services, the impact, and the expected restoration time;

(b) providing hourly updates to the Authority and customers on the progress made in resolving the faults; and

(c) submitting a formal report to the Authority within twenty-four hours of the service interruption, outlining the impact and the actions taken to restore the services.

PART VII
GENERAL PROVISIONS

23. A licensee shall-

Environmental management

(a) design and operate the data centre in a manner that maximise energy efficiency;
(b) minimise the amount of water used in cooling systems by using water conservation measures;
(c) develop a plan to reduce carbon footprint by incorporating renewable energy sources;
(d) decrease energy consumption, carbon emissions, and electronic waste by establishing energy management and sustainability plans;
(e) establish a waste management plan to handle and dispose of waste in an environmentally friendly manner; and
(f) adopt a green procurement policy to ensure that equipment, materials, and services purchased are environmentally friendly.

Penalties

24. A licensee who contravenes any provision of these Rules shall be liable to the penalty prescribed under the Act.

Dar es Salaam,
……...2026

JABIRI K. BAKARI
Director General