THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE

e-GOVERNMENT AUTHORITY

ISO 9001:2015 Certified

Document Title

Data Center Standards and Guidelines for Public Institutions

Document Number

eGA/EXT/IRA/003

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Mussa M. Kissaka	Board Chairperson		18/02/2026

Version: 2.0 – February 2026

PREFACE

Data center is a key supporting element of e-Government Initiatives and businesses for delivering services to the citizens with greater reliability, availability and serviceability. In the quest of reaping the benefits brought by the presence of Data centers, public institutions in Tanzania have vigorously been striving to take its advantage but in an uncontrolled manner that resulted into emergence of several challenges relating to collecting, storing, processing, distributing or allowing access to large amounts of data.

In the view of the above, it was apparent for enactment of the e-Government Act No. 10 of 2019 and its Regulations, 2020, which provide guidance on proper approach for implementing e-Government and establishment of e-Government Authority with mandate of coordinating, promoting and overseeing e-Government implementations as well as enforcing compliance with laws, regulations, standards and guidelines related to e-Government implementations in Public Institutions.

In this context, Section 25 (b) (ii) of the Act requires Public Institution to host the system to the Government approved hosting environment. On the same note, Section 49 requires the e-Government Authority to issue technical standards and guidelines with respect to capturing, storing, processing and sharing of electronic data. Therefore, the Authority has prepared these standards to provide a guide to public institutions upon deciding where to host Government ICT applications and not to set-up new data center. Furthermore, the standards will be used as minimum requirements in assessing the conformance of the existing data centers to be determined as approved hosting environment.

Dr. Mussa M. Kissaka

BOARD CHAIRPERSON

Table of Contents

ACRONYMS

AD	Active Directory
ATS	Automatic Transfer Switches
BoQ	Bill of Quantities
CCTV	Closed Circuit television
CRAC	Computer Room Air Conditioners
CRAH	Computer Room Air Handlers
e-GA	e-Government Authority
EOL	End Of Life
EOS	End Of Sale
GISP	Government ICT Services Portal
HVAC	Heating, Ventilation and Air Conditioning
ICT	Information and Communication Technology
ISP	Internet Service Provider
LDAP	Light Weight Directory Access Protocol
MMR	Meet Me Room
NOC	Network Operation Center
PDU	Power Distribution Unity
PLC	Program Logic Control
SCADA	Supervisory control and Data Acquisition System
SPDs	Surge-protective Devices
UPS	Uninterruptible Power Supply
VESDA	Very Early Smoke Detection Apparatus System

GLOSSARY

Civil Works	Encompasses the design, construction, and maintenance of infrastructure projects that are not typically classified as buildings. These projects include roads, bridges, railways, airports, dams, and various utilities like water and sewage systems.
Critical Data Center (Tier III)	These are Data Center facilities that accommodate systems used to deliver or perform core institutions or Government business processes.
Critical Systems	a system which is used to deliver or perform core institutions or Government business processes.
Data center	Is a dedicated space within a building, or a group of buildings used to house e-Government applications, compute, storage and networking equipment along with their supporting infrastructure.
Data Center asset database	Is an inventory of all physical and logical data center assets with key details such as description, model number, serial number, location, End of life (EOF), End of Support (EOS) etc.
Data Center Control room	Is a central space where operators monitor and manage the health, performance, and security of all data center systems and infrastructure in real-time — such as security for cybersecurity threats, compute, storage, network, power, CCTV feeds and cooling.
Meet Me Room	A secured carrier-neutral room inside data center where multiple telecommunication carriers such as Internet Service Providers (ISPs) can physically interconnect their networks.
Mission - Critical Data Center (Tier IV)	These are critical Data Centers with the highest level of fault – tolerant resilience (2N+1) such that loss, isolation, or maintenance of any one component or distribution path has zero impact on IT service.

Server Room (Tier II)	These are the ones that are responsible for hosting non-critical systems and network equipment for daily operations of an organization. The systems expected to be found within these Data Centers are meant for internal usage mainly for supporting services such as authentications (Active Directory (AD), Light-Weight Directory Access Protocol (LDAP)), file servers and network equipment.
Staging Area	Is dedicated area for unpacking, preparing, configuring, testing equipment and applications including security assessment before it's deployed in the production environment.
Truck Loading Docks	Refers to the loading delivery bays used for receiving and dispatching equipment, such as servers, racks, cooling, power and network equipment.
Utility Services	Are essential services required for operation of data center, such as electricity, water and telecommunications links.

1. INTRODUCTION

1.1 Overview

The e-Government Authority (e-GA) is an ISO 9001: 2015 certified Public Institution established under e-Government Act, 2019 mandated to coordinate, oversee, and promote e-Government initiatives as well as enforce e-Government related policies, laws, regulations, standards, and guidelines in public institutions. e-Government Authority is a succeeding institution to e-Government Agency which was a semi-autonomous institution established in 2012 under the Executive Agencies Act, No.30 Cap. 245 of 1997.

Data center is a dedicated space within a building, or a group of buildings used to house e-Government applications, compute, storage and networking equipment along with their supporting infrastructure.
The Government Data Centers can be categorized into three types according to their criticality which are Server Room (Tier II), Critical Data Center (Tier III), and Mission - Critical Data Center (Tier IV).

i. **Server Room (Tier II)**: These are the ones that are responsible for hosting non-critical systems and network equipment for daily operations of an organization. The systems expected to be found within these Data Centers are meant for internal usage mainly for supporting services such as authentications (Active Directory (AD), Light-Weight Directory Access Protocol (LDAP)), file servers and network equipment.

ii. **Critical Data Center (Tier III):** These are Data Center facilities that accommodate systems used to deliver or perform core institutions or Government business processes.

iii. **Mission - Critical Data Center (Tier IV)**: These are critical Data Centers with the highest level of fault – tolerant resilience (2N+1) such that loss, isolation, or

maintenance of any one component or distribution path has zero impact on IT service.

Data Center Standards for Public Institutions has been developed in adherence to the provisions of sections 25 (b)(ii) and 49 of the e-Government Act No. 10 of 2019 to ensure efficiency and continuous service availability for major organization applications and services that are in line with other organizations' business processes.

1.2 Purpose

This document describes standards to provide a guide to public institutions upon deciding where to host Government ICT applications and not to set-up new data center. Furthermore, the standards will be used as minimum requirements in assessing the conformance of the existing data centers to be determined as approved hosting environment.

1.3 Rationale

The choice of a proper hosting environment is not only vital to ensure compliance with relevant provisions of the e-Government Act, but it is also for ensuring continuity of business operations. To this end therefore, the Authority has developed these standards to guide all public institutions when making decisions regarding hosting of their ICT systems, compliance to which will guarantee sustainability of operations and security of their respective information.

1.4 Scope

This document will be used by all Public Institutions during decision making of host environments suitable for hosting Government ICT applications or systems.

2. GOVERNMENT DATA CENTER STANDARDS AND GUIDELINES

The Government Data Center in which public institutions host their ICT systems shall meet the following standards:

2.1 GOVERNMENT DATA CENTER STANDARDS

2.1.1 Site Selection Standards

2.1.1.1. Site Evaluation

In determining suitability of the data center site, a public institution shall ensure that: -

i. The suitability of a site is determined by a site survey, site evaluation and risk analysis.
ii. The suitability of the site is verified through obtaining official permits from relevant authority with regards to building documents, recent geological records, environmental assessment, physical security assessment or any other appropriate analytical measures.
iii. The site selection process includes a detailed analysis of all the costs associated with a particular location such as the cost to bring utilities to the site.

2.1.1.2. Hazards

Public institution shall ensure that: -

i. The choice of the location along with civil works and other installations are strategically planned to guard the data center against disasters such as floods, lighting, earthquake and fire.
ii. Seismically active areas are avoided whenever possible.
iii. A data center is located outside the immediate risk area of an active volcano.
iv. A data center is not placed on the edge of urban development or near protected natural areas.
v. The site is free of flood risk from river flood plain proximity, tidal basin proximity, dam failure, tsunami, levee failure and high crime rate.

vi. When placing a data center in close proximity to a railroad, measurement of vibration and Electromagnetic Interference (EMI) at the site is conducted over the period of three (3) to seven (7) days consecutively to aid in the assessment and mitigation requirements, if any required at the site.

2.1.1.3. Site Access and location

A public institution shall ensure that: -

i. The building is positioned at a sufficient distance from the road that a traffic accident would not cause a collision with the building itself or its external components (mechanical or electrical systems).
ii. The data center is built far from any other buildings and facilities that may pose a fire threat or that could cause damage to the data center should the other buildings or structures collapse.
iii. The disaster Recovery site is situated in a geographically separate location from the primary site and is not exposed to the same natural or man-made hazards.

2.1.1.4. Utility Services

A public institution shall ensure that:

i. Adequate electrical utility capacity to the site is provided to meet both current and projected needs of the entire site.
ii. Multiple electrical utility circuits are used, each with enough capacity to handle the entire site requirements.
iii. A data center is located in an area with easy sustainable circuit access to utility substations with preference toward an area with utility circuits provided by two or more utility substations.
iv. Utility services to the facility are routed underground whenever possible.
v. When selecting a site, ensure that there is adequate space allocated for installing one or more backup generators, one or more emergency generators, renewable energy sources (Solar) and their supporting systems.

vi. A data center is located in an area with easy sustainable connectivity to the access provider central offices preference towards an area with redundancy network connectivity.

vii. Adequate water delivery to the site is provided to meet the requirements of the data center.

viii. Sufficient water reservoir is provided for data centers.

2.1.2 Space Planning Standards

2.1.2.1. Facility Capacity

A public institution shall ensure that: -

i. The space around the data center is considered for future growth and planned easy annexation.

ii. Adequate space is provided within and between racks, the cabinet and the pathways for better cable management, bend radius protection and access.

iii. The data center has an adequately sized separate storage room for storage of items such as boxed equipment, spare air filters, spare floor tiles, spare cables, spare equipment and spare media.

2.1.2.2. Power Systems

A public institution shall ensure that: -

i. Proper grounding for both lighting protection and grid power.

ii. Adequate separation of power and telecommunications cabling are accommodated through allocating separate aisles for power and telecommunications cabling in the main aisles.

iii. Vertical separation is provided by placing the telecommunications cabling in cable trays or baskets as far as above the power cables.

iv. Planning for overhead cable trays for telecommunications cabling is coordinated with architects, mechanical engineers and electrical engineers that are designing lighting, plumbing, air ducts, power and fire protection systems.

2.1.2.3. Cooling Capacity

A public institution shall ensure that: -

i. There is adequate cooling equipment that includes energy efficient units such as in-row cooling system, rear door heat exchangers or direct to cheap liquid cooling.
ii. It employs raised floor plenum or overhead cable tray for more flexible cooling.
iii. The cabinets and racks are arranged in an alternating pattern to create hot and cold aisle.
iv. The air conditioning system is designed to provide the design temperature and humidity conditions recommended by the manufacturers of the services to be installed within the data center.

2.1.2.4. Physical Security

A public institution shall ensure that: -

i. Truck loading docks is provided as required to handle anticipated deliveries and shall be provided with a level of security similar to the other building entrances.
ii. The data center is located inside the existing building so that there are no exterior windows or doors.
iii. In situations where you must share data center space with other institutions, an effective means of segregating the space should be considered.

2.1.2.5. Data Center Supporting Spaces

A public institution shall ensure that;

i. Support equipment such as HVAC Outdoor Unit, UPS battery backup and generators is located outside of the data center IT room.
ii. There is dedicated staging area for unpacking, preparing, configuring, testing equipment and applications including security assessment before it's deployed in the production environment.
iii. It has a Meet-Me Rooms (MMRs) in a data center to ensure multiple telecommunication carriers such as Internet Service Providers (ISPs) can physically interconnect their networks.

iv. For Mission Critical Data Center (Tier IV), it has two physically diverse meet-me rooms minimizing the risk of downtime due to a single point of failure.

2.1.3 Architectural Standards

2.1.3.1. General Design Concepts

A public institution shall ensure that: -

i. A data center is designed with plenty of flexible white space that can accommodate future racks or cabinets.
ii. The 'as built' physical and logical designs of the data center including architectural, structural, network, electrical and mechanical designs are documented.
iii. Physical and logical designs are updated whenever changes occur.
iv. The network design is segmented to isolate different types of data center traffic such as computing traffic, surveillance camera feeds and access control system.
v. Data center design is developed with associated specifications and Bill of Quantities (BoQ).
vi. A data center has been designed to accommodate diverse hardware designs and requirements, and equipment from different manufacturers.
vii. The data center design supports future scalability and modular growth without requiring complete infrastructure overhaul.
viii. The data center has been designed to limit and control access.
ix. A data center has a single point of entry and sufficient set back of building for perimeter security purposes.
x. For Server Room (Tier II), there should be redundancy of (N+1) capacity in some components including power, cooling, network equipment's, and Internet Service Provider (ISP).
xi. For Critical Data Center (Tier III), there should be minimum redundancy of (N+1) capacity in all components including uninterruptable power supply (UPS), ICT infrastructure, auxiliary generator, cooling and Internet Service Provider (ISP).
xii. For Mission - Critical Data Center (Tier IV), there should be minimum redundancy of 2N+1 capacity in all components including uninterruptable power supply

(UPS), ICT infrastructure, auxiliary generator, cooling and Internet Service Provider (ISP).

2.1.3.2. Construction Components

A public institution shall ensure that: -

i. The building structural system is made of steel or concrete or fabricated material. At a minimum, the building frame shall be designed such that it can withstand wind loads in accordance with applicable building codes for relevant institutions charged with building approvals.
ii. Floors, walls and ceiling are sealed, painted or constructed of a material to minimize dust.
iii. Walls, floors and ceilings are light in colour to enhance room lighting.

2.1.4 Mechanical Systems Standards

A public institution shall ensure that: -

i. The main facility is equipped with HVAC system to manage thermos load and maintain optimal humidity for data center equipment's.
ii. It has installed multiple HVAC systems for redundancy as opposed to relying on a single centralized chiller.
iii. An ambient temperature within the data center is between 18 and 23 degrees Celsius. Further consideration should be emphasized on specified equipment temperature range for optimum operation as recommended by manufacturer.
iv. A relative humidity of 45 percent to 50 percent is maintained within the data center. Further consideration should be emphasized on specified equipment humidity range for optimum operation as recommended by manufacturer.
v. The airflow is designed to maximize the flow of chilled air across and through the equipment racks. This requires that chilled air flow from bottom to top and from front to back through the racks.
vi. Alternate aisles between cold-aisle and hot aisle facilitates a more-efficient temperature control.

vii. It maintains a static pressure within the raised floor plenum of 5 percent greater than the data center raised-floor area such as ensuring consistent and efficient airflow distribution to the IT equipment's.

viii. It selectively positions perforated tiles in the raised floor to direct chilled air into the rack area.

ix. It seals all penetrations in the raised floor to maintain a constant static pressure.

x. It establishes a vapour barrier throughout the perimeter of the data center to minimize condensation.

xi. Use spot cooling or special rack enclosures for hot spots in the data center layout.

2.1.5 Electrical Systems Standards

2.1.5.1. Main and step-down transformers

A public institution shall ensure that a transformer: -

i. Is located in a secure mechanical room.

ii. Is installed in a separate room with adequate ventilation to support sufficient heat dissipation and maintain operational integrity.

iii. Is maintained by a qualified technician to factory standards and be supportable by extended factory warranty.

2.1.5.2. Main power control panel and Programmable Logic Control (PLC)

(a) A public institution shall ensure that main power control panel and PLC: -

i. Are installed and located in a secure mechanical room.

ii. Are administered and maintained by a qualified technician to factory standards.

iii. Have HVAC systems to support heat load and correct humidity levels for each unit.

(b) A public institution shall ensure that PLC: -

i. Have password security.

ii. Have UPS support for power failure.

iii. Supports seamless communications with systems such as Building Management System (BMS), Data Center Infrastructure Management System (DCIMS), Supervisory control and Data Acquisition System (SCADA).

2.1.5.3. Backup batteries

A public institution shall ensure that backup batteries: -

i. Are eco-friendly and installed, operated, and maintained by authorized technician whilst adhering to manufacture's recommendations for system to be of sufficient quality and capacity to ensure a long life.
ii. Are located in secure area with proper ventilation as required.
iii. Are approved for use in computer equipment UPS systems.
iv. Facilities can sustain the expected load capacity for at least one (1) hour on total power blackout.

2.1.5.4. UPS systems

A public institution shall ensure that UPS systems: -

i. Are located in a secure area with proper ventilation as required.
ii. Are eco-friendly, installed, operated, and maintained by authorized technician whilst adhering to manufacture's recommendations.
iii. Have sufficient backup battery to meet current and future needs to allow for a controlled shutdown of servers in the event of power blackout.
iv. Have bypass capability to allow for periodic maintenance.
v. Are designed in redundant to provide non disruption of services during maintenance.
vi. Provides a dedicated backup power source for critical safety systems such as emergency lighting, CCTV Camera and fire-alarm panels.

2.1.5.5. Generator management

A public institution shall ensure that: -

i. Are located in a secure area with proper ventilation as required.
ii. Generators are tested and run for at least one hour in every month.
iii. A full load test and switching test is conducted at least yearly.
iv. Maintenance logs are kept on all tests and reflect all maintenance performed.
v. Server Room (Tier II) is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HVAC) for not less than twelve (12) hours.

vi. Critical Data Center (Tier III) is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HVAC) for not less than seventy-two (72) hours.

vii. Mission - Critical Data Centers (Tier IV) is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HVAC) for not less than ninety – six (96) hours.

viii. All maintenances are performed by a qualified technician to factory specifications.

ix. Generator Management includes remote alarm panel (annunciator panel) and fuel monitoring capability.

x. It has an automatic transfer switch (ATS).

xi. For Mission Critical Data Center (Tier IV), it has redundant automatic-transfer-switch (ATS).

2.1.5.6. Power strips

A public institution shall ensure that: -

i. Power strips are sized to meet the power requirements of the cabinet in which they are installed.

ii. Power receptacles for power strips are installed by qualified electricians.

2.1.5.7. Power cable layout

A public institution shall ensure that: -

i. Equipment power cables are within the minimum required length and slack/strain management are employed.

ii. Power cables are aligned to minimize air flow disruptions.

iii. Power cables are labelled.

2.1.5.8. Grounding systems

A public institution shall ensure that: -

i. Data center equipment grounds are independent of all other building grounds (such as lightning protection systems).

ii. All metal objects are bonded to the ground including cabinets, racks, PDUs, HVACs, cable pathway, and any raised floor systems.

iii. Ground resistance is less than five (5) Ohm.

2.1.5.9. Surge Protection and Voltage Regulation

A public institution shall ensure that: -

i. Implements properly rated surge-protective devices (SPDs) to all power components including main power control panel, Input and Output Power Distribution Unit (PDU), Uninterrupted Power Supply (UPS), and cooling equipment's.

ii. Has an automatic-voltage-regulation (AVR) system to correct sustained over-voltage or under-voltage conditions.

2.1.6 Cabling Infrastructure Standards

2.1.6.1. Overhead delivery system cable layout

A public institution shall ensure that the IT room has a system to support overhead delivery of data connections to the equipment cabinets.

2.1.6.2. Fiber and copper cable standards

A public institution shall ensure that: -

i. Fiber installation uses multimode (OM4/OM5) or single mode (OS1/OS2) Laser optimized fiber.
ii. All fiber installations and copper data cables are labeled.
iii. Copper jumpers are of CAT6/CAT7 with Booted RJ45 connectors.
iv. Fiber and copper cables are within the minimum required length and slack/strain management are employed.
v. Cables are aligned to minimize air flow disruptions.
vi. Fiber and copper cables are periodically tested to verify their reliability and performance.

2.1.7 Fire Protection Standards

2.1.7.1. Fire Detection Standards

A public institution shall ensure that: -

i. The fire detection system is designed specifically for use in data centers.
ii. The fire detection system is installed and tested in conformance to applicable local and international fire requirements.
iii. The fire detection system is maintained by qualified technicians.
iv. Detectors include both heat and smoke-sensing devices such as Very Early Smoke Detection Apparatus System (VESDA) and be interconnected with the fire suppression system, local alarms, and local or central monitoring stations.
v. The detectors are positioned in relation to airflow patterns to ensure early detection of an imminent electrical fire.
vi. A separate fire alarm panel is deployed for Data Center area.
vii. The deployed fire alarm panel communicates the alarm signal to the master fire panel that monitors the entire premise.
viii. The deployed fire alarm panel has the capability to send audio/visual signal at security area or Data Center Control Room.

For data center employing raised-floor plenum, smoke-detection devices shall be installed beneath the raised floor to provide full coverage of the white-space sub-floor area.

2.1.7.2. Fire Suppression Standards

A public institution shall ensure that: -

i. The fire suppression system is designed specifically for use in data centers.
ii. The fire suppression system is installed and tested in conformance to applicable local and international fire requirements.
iii. The fire suppression system is maintained by qualified technicians.
iv. The installation of fire-rated walls, doors and ceiling is in accordance with the relevant standards such as NFPA 75.
v. The use of a chemical or "clean agent" suppression system is the first line of defense to ensure no damage to sensitive equipment's and harm to building occupants.

vi. The installation of a fire sprinkler system is either a pre-action or flooded system for areas excluding IT, power and mechanical rooms.
vii. Manual systems, including manual pull stations and portable fire extinguishers are appropriately positioned throughout the data center.
viii. Fire suppression systems are securely and properly mounted.

2.1.8 Security Standards

2.1.8.1. Door security

A public institution shall ensure that: -

i. Door access control is maintained 24/7.
ii. An electronic access control system is in place.
iii. Electronic access control system is implemented with multi-factor authentication for critical and mission - critical data centers (Tier III and IV).
iv. The electronic access control system has the capability to record access to all secure data center areas and retains those logs for a minimum of one year.
v. Enforcement of strict policies and sign in/out logs are mandatory.
vi. Review of procedures and sign in/out logs are done on a regular basis.
vii. Secured doors are fail open in a fire emergency.

2.1.8.2. Video surveillance

A public institution shall ensure that: -

i. CCTV cameras cover all the area in the Data center for monitoring real time movements within the Data center.
ii. Local and remote surveillance of secured and public spaces is allowed.
iii. Recording devices (tape or hard disk) are located in a secure area.
iv. Review of the recordings is done on a regular basis to ensure proper operation of the video security system.
v. All security recordings are saved for not less than 90 days.

2.1.8.3. Granting security access

A public institution shall ensure that: -

i. Data center locations have a visitor/non-essential staff access policy.
ii. Access must only be granted to essential personnel.
iii. Visitors are signed in and out and are always supervised.
iv. Visitor logs are maintained for a minimum of one year.

2.1.8.4. Emergency procedures

A public institution shall ensure that: -

i. All sites maintain published emergency procedures including fire Evacuation Plan and emergency contact information.
ii. It performs regular emergency procedures awareness, trainings and testing as per the institutional Business Continuity Plan (BCP).
iii. Exit routes are clearly marked with illuminated or photoluminescent signage placed across the facility to ensure safe and efficient evacuation.

2.1.8.5. ICT Security

A public institution shall ensure that all data center infrastructure and operations comply with the e-Government Security Architecture Standards and Technical Guidelines (eGA/EXT/ISA/001).

2.1.9 Monitoring Standards

A public institution shall ensure that: -

i. All data center systems and infrastructure are monitored regularly.
ii. For critical and mission - critical data centers (Tier III and IV), monitoring system for all installed equipment are installed in one centralized panel at Data Center Control Room.
iii. Sensing cables are installed along room perimeter, under the raised floor, as well as areas prone to water leakage such as HVAC units and water pipes.

iv. Air conditioning systems are specifically designed for stringent environmental control with automatic monitoring and control of cooling, heating, humidification, dehumidification, and air filtration function.
v. Data Center Control Room is provided with a separate air conditioning system so that the air conditioning units can be switched off whenever needed.
vi. Access to the Data center room is controlled using access control system limited to only staffs who are responsible for managing and operating the Data center infrastructure.
vii. The Data Center asset database is in place and updated whenever changes occur.

2.1.10 Maintenance Standards

2.1.10.1. Preventive maintenance

Public institution shall ensure that all equipment undergo preventive maintenance quarterly or as per manufacturer requirements, whichever is more stringent.

2.1.10.2. Building

A public institution shall: -

i. Check the condition of floors, ceilings, and walls including leakage or damage and carry out necessary repairs.
ii. Make sure that exits are clearly marked, with additional signage as needed.
iii. Make sure that data center is free of trash or large items that could be a fire or tripping hazard.
iv. Conduct routine pest inspections and treatments.

2.1.10.3. ICT Equipment

A public institution shall ensure that: -

i. ICT hardware equipment i.e. servers, communication gear, and storage equipment are racked in appropriate locations as per plan.
ii. There is no loose wire on or above the floor.

iii. The asset management database is used to create a removal list of all hardware, power, and connections related to the server(s).
iv. All equipment to be removed are powered down before removal.
v. All servers and components to be removed are labeled, inventoried, and properly bundled for delivery to owner or disposal.
vi. Blanking panels are installed in the vacated rack space.

2.1.10.4. Documentation

A public institution shall ensure that: -

i. A change request documenting additional or removal is completed and approved before work begins.
ii. The Data Center asset database and all other records relating to the equipment are updated to reflect the change.

2.1.10.5. Disposition

A public institution shall ensure that: -

i. The disposition of the server after removal are documented before the process starts.
ii. All components are inventoried and a list created for the history file and turnover to client or for disposal.
iii. All Institution's asset removal/repurpose forms are completed.
iv. All items are processed in accordance with the Public Finance (Management of Public Property) Regulations, 2024 and the Electronic and Postal Communication (Electronic Communications Equipment Standards and E-Waste Management) (Amendments) Regulations, 2024.

2.1.10.6. Electrical Infrastructure

A public institution shall ensure that: -

i. All electrical system components are regularly inspected and carry out necessary repairs.
ii. Backup generators are available and are in good working order.

iii. Automatic Transfer Switches (ATS), Uninterrupted Power Supplies (UPS), and Power Distribution Units (PDU) are in good working order.
iv. The PDU/Wall Breaker Panel map are updated.
v. All unused or decommissioned power, data circuits, management circuits, and fiber connections are reclaimed and removed.
vi. All breakers are turned off during maintenance of electrical equipment.

2.1.10.7. Cooling Infrastructure

A public institution shall: -

i. Check and confirm that Computer Room Air Conditioners (CRAC) or Computer Room Air Handlers (CRAH) and the overall HVAC system is efficiently functional regularly.
ii. Replaces filters based on operational hours, manufacturer guidance or pressure drop-readings.
iii. Clean evaporator coils regularly and ensure proper air filtration upstream.
iv. Regularly inspect and adjust belt tension to the manufacturers recommended specifications.

2.1.10.8. Security and Safety

A public institution shall: -

i. Check the locks and the doors, make sure that they lock and unlock easily.
ii. Test smoke and carbon monoxide detectors and change batteries at least twice a year.
iii. Check that all lights (interior and exterior) are working, replacing bulbs as needed.
iv. Regularly check the visitors' list and try to limit access to the data center as much as possible.
v. Check the surveillance system is in good working order.

2.1.10.9. Cleaning

A public institution shall: -

i. Check the cleanliness condition of the data center facility.
ii. Make sure that the data center hardware equipment and the facility itself is free of dust and contamination.

2.1.11 Operation standards

2.1.11.1. Service Level Agreement

A public institution shall ensure that: -

i. Services within the data center are maintained with the minimum service availability of:
    a. 99.741% (22 hours of downtime annually) for Server Room (Tier II).
    b. 99.982% (1.6 hours of downtime annually) for Critical Data Centers (Tier III).
    c. 99.995% (26.3 minutes of downtime annually) for Mission Critical Data Centers (Tier IV).

2.1.11.2. Testing

All components of the data center facility are periodically tested to ensure that they function properly. Records for these reports shall be kept appropriately.

2.1.11.3. Operations management

Public institution shall: -

i. Establish a standard operating procedures for data center operations.
ii. Clearly define roles and responsibilities for data center personnel.

2.1.11.4. Incident management

Public institution shall: -

i. Establish process and procedures for incident management, disaster recovery and business continuity.
ii. Ensure it tests the incident management plan, disaster recovery plan and business continuity plan.

2.1.11.5. Capacity management

Public institution shall: -

i. Ensure the data center has sufficient capacity across computer, power, cooling, storage, networking, white space, and management infrastructure to reliably meet current and future demands.
ii. Prepare capacity analysis reports quarterly.

2.2 GOVERNMENT DATA CENTER GUIDELINES

Public institution shall ensure that: -

i. It refers to Appendix I, to guide the mapping of applicable data center standards and determine the most suitable type of Government Data Centre for their needs.
ii. All data center equipment is procured through the Government Procurement processes in accordance with Tanzania Public Procurement Act and its regulations.
iii. The institutional training plan includes relevant trainings on data center operations and ensures that they are performed regularly.
iv. All equipment undergoes preventive maintenance quarterly or as per manufacturer requirements, whichever is more stringent.
v. For deployment of stand-alone of e-Government shared system, Critical Data Center (Tier III) requirements must be met.
vi. They adhere to the "Data Center Standards" as a minimum requirement upon deciding where to host Government ICT applications and not to set-up new data center.
vii. All data center equipment is selected with preference to environmental friendliness, energy efficient and sustainable technologies.
viii. If intends to provide data center services (co-location, co-hosting) to other public institutions must first obtain approval from the Authority.
ix. Reviews the availability and effectiveness of cooling and power capacity prior to any ICT equipment changes.
x. For critical and mission - critical data centers (Tier III and IV), monitors security and data center components such as compute, storage, network, cooling, and power in 24/7.

xi. Test environment and production environment are physically and/or logically segmented.

xii. Both Primary and Disaster recovery sites meet the data center standards with respect to the criticality of the hosted system.

xiii. Does not use equipment that has reached end of support (EOS) and end of life (EOL).

xiv. Regularly perform redundancy testing to validate fail over capabilities to all data center components such as computing, storage, power, cooling and network.

xv. All data center ICT assets such as network appliances, systems, applications, storage devices and data are identified, classified, managed and reported to the Authority through the Government ICT Service Portal (GISP).

xvi. It does not host in non-Government owned cloud platform.

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

This document shall be:

3.1 Effective upon being reviewed and approved by the Authority Board of Directors.

3.2 Subjected to review at least once every three years or whenever necessary changes are needed.

3.3 Continually complied to and any exception to its application must be duly authorized.

4. RELATED DOCUMENTS

4.1. e-Government Act No.10 of 2019.

4.2. e-Government Regulations 2020.

4.3. e-Government Infrastructure Architecture Standards and Technical guidelines (eGA/EXT/IRA/001).

4.4. e-Government Security Architecture Standards and Technical Guidelines (eGA/EXT/ISA/001).

4.5. e-Government Guideline (PO-PSM, 2017).

4.6. Telecommunication infrastructure standard for data centers (TIA-942)

4.7. Information Technology – Data Center Facilities and Infrastructure (ISO/IEC TS 22237).

4.8. National Fire Protection Association Standards - NFPA 75.

4.9. American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Standards and Guidelines.

4.10. Minimum Technical Specifications for Data Center (TCRA/TS013).

4.11. TIA-568.2-D Level 2G.

4.12. Public Finance (Management of Public Property) Regulations, 2024

4.13. Electronic and Postal Communication (Electronic Communications Equipment Standards and E-Waste Management) (Amendments) Regulations, 2024.

4.14. Guidelines and Criteria for Cloud and Stand-alone Deployment of e-Government Shared Systems.

4.15. Standards and Guidelines for ICT Readiness in Government Owned

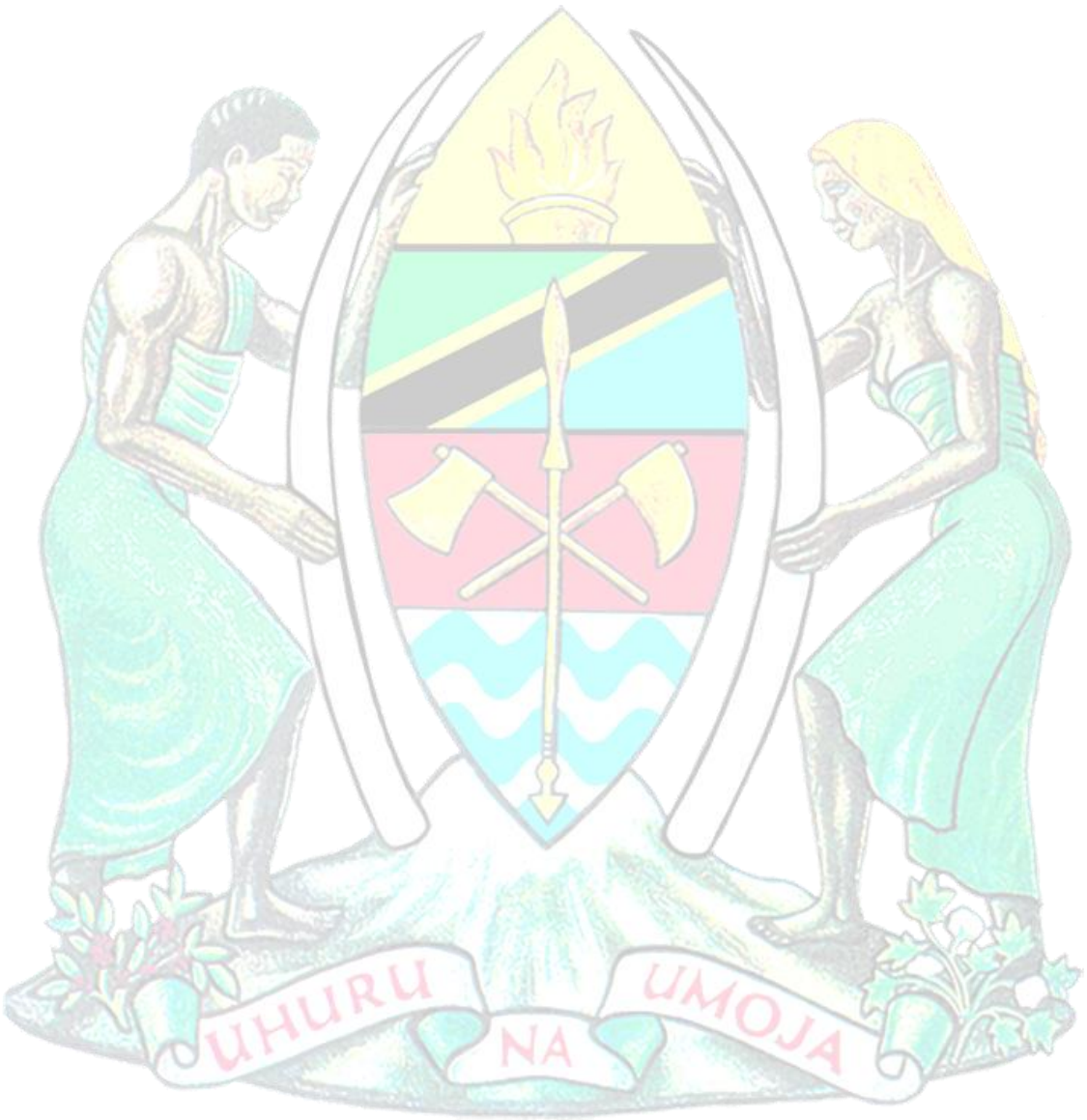
4.16. Infrastructure.

4.17. Data Center Site Infrastructure Tier Standard: Topology.

5. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	e-GA	Creation of Document	December 2020
Ver. 2.0	e-GA	-Changes to definition of Data Center Categories. -Addition of "Section 2.1.11. Operation Standards". -Addition of "Section 2.2. Data Center Guidelines." - All Standards Sections Update such as Site Selection Standards, Planning, Architectural. - Inclusion of energy efficient equipment. - Handling of e-Waste in accordance with Electronic and Postal Communication (Electronic	February 2026

		Communications Equipment Standards and E-Waste Management) (Amendments) Regulations.	



APPENDIX

Appendix I describes the mapping between the above standards and types of Government Data Centers.

Appendix I: Standards requirements for different Government Data Centers

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
1.	**Site Selection Standards**				
1.1.	Site Evaluation	The suitability of a site is determined by a site survey, site evaluation and risk analysis.	√	√	√
1.2		The suitability of the site is verified through obtaining official permits from relevant authority with regards to building documents, recent geological records, environmental assessment, physical security assessment or any other appropriate analytical measures.	√	√	√
1.3		The site selection process includes a detailed analysis of all the costs associated with a particular location such as the cost to bring utilities to the site.	√	√	√
1.4	Hazards	The choice of the location along with civil works and other installations are strategically planned to guard the data center against disasters such as floods, lighting, earthquake and fire.	√	√	√
1.5		Seismically active areas should be avoided whenever possible.	√	√	√
1.6		A data center is located outside the immediate risk area of an active volcano.	√	√	√
1.7		A data center is not placed on the edge of urban development	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		or near protected natural areas.			
1.8		The site is free of flood risk from river flood plain proximity, tidal basin proximity, dam failure, tsunami, levee failure and high crime rate.	√	√	√
1.9		When placing a data center in close proximity to a railroad, measurement of vibration and Electromagnetic Interference (EMI) at the site is conducted over the period of three (3) to seven (7) days consecutively to aid in the assessment and mitigation requirements, if any required at the site.	√	√	√
1.10	Site Access and location	The building is positioned at a sufficient distance from the road that a traffic accident would not cause a collision with the building itself or its external components (mechanical or electrical systems).	√	√	√
1.11		The data center is built far from any other buildings and facilities that may pose a fire threat or that could cause damage to the data center should the other buildings or structures collapse.	√	√	√
1.12		The disaster Recovery site is situated in a geographically separate location from the primary site and is not exposed to the same natural or man-made hazards.	√	√	√
1.13	Utility Services	Adequate electrical utility capacity to the site is provided to meet both current and	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		projected needs of the entire site.			
1.14		Multiple electrical utility circuits are used, each with enough capacity to handle the entire site requirements.	√	√	x
1.15		A data center is located in an area with easy sustainable circuit access to utility substations with preference toward an area with utility circuits provided by two or more utility substations.	√	√	x
1.16		Utility services to the facility are routed underground whenever possible.	√	√	√
1.17		When selecting a site, ensure that there is adequate space allocated for installing one or more backup generators, one or more emergency generators, renewable energy sources (Solar) and their supporting systems.	√	√	x
1.18		A data center is located in an area with easy sustainable connectivity to the access provider central offices preference towards an area with redundancy network connectivity.	√	√	√
1.19		Adequate water delivery to the site is provided to meet the requirements of the data center.	√	√	√
1.20		Sufficient water reservoir is provided for data centers.	√	√	√
2.	**Space Planning Standards**				
2.1	Facility Capacity	The space around the data center is considered for future	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		growth and planned easy annexation.			
2.2		Adequate space is provided within and between racks, the cabinet and the pathways for better cable management, bend radius protection and access.	√	√	√
2.3		The data center has an adequately sized separate storage room for storage of items such as boxed equipment, spare air filters, spare floor tiles, spare cables, spare equipment and spare media.	√	√	√
2.4	Power Systems	Proper grounding for both lighting protection and grid power.	√	√	√
2.5		Adequate separation of power and telecommunications cabling are accommodated through allocating separate aisles for power and telecommunications cabling in the main aisles.	√	√	√
2.6		Vertical separation is provided by placing the telecommunications cabling in cable trays or baskets as far as above the power cables.	√	√	√
2.7		Planning for overhead cable trays for telecommunications cabling is coordinated with architects, mechanical engineers and electrical engineers that are designing lighting, plumbing, air ducts, power and fire protection systems.	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
2.8	Cooling Capacity	There is adequate cooling equipment that includes energy efficient units such as in-row cooling system, rear door heat exchangers or direct to cheap liquid cooling.	√	√	√
2.9		It employs raised floor plenum or overhead cable tray for more flexible cooling.	√	√	√
2.10		The cabinets and racks are arranged in an alternating pattern to create hot and cold aisle.	√	√	x
2.11		The air conditioning system is designed to provide the design temperature and humidity conditions recommended by the manufacturers of the services to be installed within the data center.	√	√	√
2.12	Security	Truck loading docks is provided as required to handle anticipated deliveries and shall be provided with a level of security similar to the other building entrances.	√	√	√
2.13		The data center is located inside the existing building so that there are no exterior windows or doors.	√	√	√
2.14		In situations where you must share data center space with other institutions, an effective means of segregating the space should be considered.	√	√	√
2.15	Data Center Supporting Spaces	Support equipment such as HVAC Outdoor Unit, UPS battery backup and generators is located outside of the data center IT room.	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
2.16		There is dedicated staging area for unpacking, preparing, configuring, testing equipment and applications including security assessment before it's deployed in the production environment.	√	√	x
2.17		It has a Meet-Me Rooms (MMRs) in a data center to ensure multiple telecommunication carriers such as Internet Service Providers (ISPs) can physically interconnect their networks.	√	√	x
2.18		For Mission Critical Data Center (Tier IV), it has two physically diverse meet-me rooms minimizing the risk of downtime due to a single point of failure.	√	x	x
3.	**Architectural Standards**				
3.1	General Design Concepts	A data center is designed with plenty of flexible white space that can accommodate future racks or cabinets.	√	√	√
3.2		The 'as built' physical and logical designs of the data center including architectural, structural, network, electrical and mechanical designs are documented.	√	√	√
3.3		Physical and logical designs are updated whenever changes occur.	√	√	√
3.4		The network design is segmented to isolate different types of data center traffic such as computing traffic, surveillance camera feeds and access control system.	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
3.5		Data center design is developed with associated specifications and Bill of Quantities (BoQ).	√	√	√
3.6		A data center has been designed to accommodate diverse hardware designs and requirements, and equipment from different manufacturers.	√	√	√
3.7		The data center design supports future scalability and modular growth without requiring complete infrastructure overhaul.	√	√	√
3.8		The data center has been designed to limit and control access.	√	√	√
3.9		A data center has a single point of entry and sufficient set back of building for perimeter security purposes.	√	√	√
3.10		For Server Room (Tier II), there should be redundancy of (N+1) capacity in some components including power, cooling, network equipment's, and Internet Service Provider (ISP).	x	x	√
3.11		For Critical Data Center (Tier III), there should be minimum redundancy of (N+1) capacity in all components including uninterruptable power supply (UPS), ICT infrastructure, auxiliary generator, cooling	x	√	x

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		and Internet Service Provider (ISP).			
3.12		For Mission - Critical Data Center (Tier IV), there should be minimum redundancy of 2N+1 capacity in all components including uninterruptable power supply (UPS), ICT infrastructure, auxiliary generator, cooling and Internet Service Provider (ISP).	√	x	x
3.13	Construction Components	The building structural system is made of steel or concrete. At a minimum, the building frame shall be designed such that it can withstand wind loads in accordance with applicable building codes for relevant institutions charged with building approvals.	√	√	√
3.13		Floors, walls and ceiling are sealed, painted or constructed of a material to minimize dust.	√	√	√
3.14		Walls, floors and ceilings are light in colour to enhance room lighting.	√	√	√
4.	**Mechanical Systems Standards**				
4.1		The main facility is equipped with HVAC system to manage thermos load and maintain optimal humidity for data center equipment's.	√	√	√
4.2		It has installed multiple HVAC systems for redundancy as opposed to relying on a single centralized chiller.	√	√	x

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
4.3		An ambient temperature within the data center is between 18 and 23 degrees Celsius. Further consideration should be emphasized on specified equipment temperature range for optimum operation as recommended by manufacturer.	√	√	√
4.4		A relative humidity of 45 percent to 50 percent is maintained within the data center. Further consideration should be emphasized on specified equipment humidity range for optimum operation as recommended by manufacturer.	√	√	√
4.5		The airflow is designed to maximize the flow of chilled air across and through the equipment racks. This requires that chilled air flow from bottom to top and from front to back through the racks.	√	√	x
4.6		Alternate aisles between cold-aisle and hot aisle facilitates a more-efficient temperature control.	√	√	x
4.7		It maintains a static pressure within the raised floor plenum of 5 percent greater than the data center raised-floor area such as ensuring consistent and efficient airflow distribution to the IT equipment's.	√	√	√
4.8		It selectively positions perforated tiles in the raised floor to direct chilled air into the rack area.	√	√	x

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
4.9		It seals all penetrations in the raised floor to maintain a constant static pressure.	√	√	x
4.10		It establishes a vapour barrier throughout the perimeter of the data center to minimize condensation.	√	√	x
4.11		Use spot cooling or special rack enclosures for hot spots in the data center layout.	√	√	x
5.	**Electrical Systems Standards**				
5.1	Main and step-down transformers	Has been located in a secure mechanical room.	√	√	x
5.2		Is installed in a separate room with adequate ventilation to support sufficient heat dissipation and maintain operational integrity.	√	√	x
5.3		Is maintained by a qualified technician to factory standards and be supportable by extended factory warranty.	√	√	x
5.4	Main power control panel and PLC	Are installed and located in a secure mechanical room.	√	√	x
5.5		Are administered and maintained by a qualified technician to factory standards.	√	√	x
5.6		Have HVAC systems to support heat load and correct humidity levels for each unit.	√	√	x
5.7		PLC has password security.	√	√	x
5.8		PLC has UPS support for power failure.	√	√	x
5.9		Supports seamless communications with systems such as Building Management System (BMS), Data Center Infrastructure Management System (DCIMS), Supervisory	√	x	x

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		control and Data Acquisition System (SCADA).			
5.10	Backup Batteries	Are eco-friendly and installed, operated, and maintained by authorized technician whilst adhering to manufacture's recommendations for system to be of sufficient quality and capacity to ensure a long life.	√	√	√
5.11		Are located in secure area with proper ventilation as required.	√	√	√
5.12		Are approved for use in computer equipment UPS systems.	√	√	√
5.13		Facilities are able to sustain the expected load capacity for at least one (1) hour on total power blackout	√	√	√
5.14	UPS Systems	Are located in a secure area with proper ventilation as required.	√	√	√
5.15		Are eco-friendly, installed, operated, and maintained by authorized technician whilst adhering to manufacture's recommendations.	√	√	√
5.16		Have sufficient backup battery to meet current and future needs to allow for a controlled shutdown of servers in the event of power blackout.	√	√	√
5.17		Have bypass capability to allow for periodic maintenance.	√	√	√
5.18		Are designed in redundant to provide non disruption of services during maintenance.	√	√	√
5.19		Provides a dedicated backup power source for critical safety systems such as emergency	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		lighting, CCTV Camera, and fire-alarm panels.			
5.20	Generator Management	Are located in a secure area with proper ventilation as required.	√	√	x
5.21		Generators are tested and run for at least one hour in every month.	√	√	x
5.22		A full load test and switching test is conducted at least yearly.	√	√	x
5.23		Maintenance logs are kept on all tests and reflect all maintenance performed.	√	√	x
5.24		Server Room (Tier II) is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HVAC) for not less than twelve (12) hours.	√	√	x
5.25		Critical Data Center (Tier III) is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HVAC) for not less than seventy-two (72) hours.	x	√	x
5.26		Mission - Critical Data Centers (Tier IV) is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HVAC) for not less than ninety – six (96) hours.	√	x	x
5.27		All maintenances are performed by a qualified technician to factory specifications.	√	√	x

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
5.28		Generator Management includes remote alarm panel (annunciator panel) and fuel monitoring capability.	√	√	x
5.29		It has an automatic transfer switch (ATS).	√	√	√
5.30		For Mission Critical Data Center (Tier IV), it has redundant automatic-transfer-switch (ATS).	√	x	x
5.31	Power strips	Power strips are sized to meet the power requirements of the cabinet in which they are installed.	√	√	√
5.32		Power receptacles for power strips are installed by qualified electricians.	√	√	√
5.33	Power cable layout	Equipment power cables are within the minimum required length and slack/strain management are employed.	√	√	√
5.34		Cables are aligned to minimize air flow disruptions.	√	√	√
5.35		Power cables are labelled.	√	√	√
5.36	Grounding Systems	Data center equipment grounds are independent of all other building grounds (such as lightning protection systems).	√	√	x
5.37		All metal objects are bonded to the ground including cabinets, racks, PDUs, HVACs, cable pathway, and any raised floor systems.	√	√	√
5.38		Ground resistance is less than five (5) Ohm.	√	√	√
5.39	Surge Protection and	Implements properly rated surge-protective devices (SPDs) to all power components including main	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
	Voltage Regulation	power control panel, Input and Output Power Distribution Unit (PDU), Uninterrupted Power Supply (UPS), and cooling equipment's.			
5.40		Has an automatic voltage regulation (AVR) system to correct sustained over voltage or under voltage conditions.	√	√	x
6.	**Cabling Infrastructure Standards**				
6.1	Overhead delivery system cable layout	A public institution shall ensure that the IT room has a system to support overhead delivery of data connections to the equipment cabinets.	√	√	√
6.2	Fiber and copper cable Standards	Fiber installation uses multimode (OM4/OM5) or single mode (OS1/OS2) Laser optimized fiber.	√	√	√
6.3		All fiber installations and copper data cables are labeled.	√	√	√
6.4		Copper jumpers are of CAT6/CAT7 with Booted RJ45 connectors.	√	√	√
6.5		Fiber and copper cables are within the minimum required length and slack/strain management are employed	√	√	√
6.6		Cables are aligned to minimize air flow disruptions.	√	√	√
6.7		Fiber and copper cables are periodically tested to verify their reliability and performance	√	√	√
7.	**Fire Protection Standards**				
7.1	Fire Detection Standards	The fire detection system is designed specifically for use in data centers.	√	√	√
7.2		The fire detection system is installed and tested in conformance to applicable	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		local and international fire requirements.			
7.3		The fire detection system is maintained by qualified technicians.	√	√	√
7.4		Detectors include both heat and smoke-sensing devices such as Very Early Smoke Detection Apparatus System (VESDA) and be interconnected with the fire suppression system, local alarms, and local or central monitoring stations.	√	√	√
7.5		The detectors are positioned in relation to airflow patterns to ensure early detection of an imminent electrical fire.	√	√	√
7.6		A separate fire alarm panel is deployed for Data Center area.	√	√	√
7.8		The deployed fire alarm panel communicates the alarm signal to the master fire panel that monitors the entire premise.	√	√	√
7.9		The deployed fire alarm panel has the capability to send audio/visual signal at security area or Data Center Control Room.	√	√	√
7.10		For data center employing raised-floor plenum, smoke-detection devices shall be installed beneath the raised floor to provide full coverage of the white-space sub-floor area.	√	√	√
7.11	Fire Suppression Standards	The fire suppression system is designed specifically for use in data centers.	√	√	√
7.12		The fire suppression system is installed and tested in	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		conformance to applicable local and international fire requirements.			
7.13		The fire suppression system is maintained by qualified technicians.	√	√	√
7.14		The installation of fire-rated walls, doors and ceiling is in accordance with the relevant standards such as NFPA 75.	√	√	√
7.15		The use of a chemical or "clean agent" suppression system is the first line of defense to ensure no damage to sensitive equipment's and harm to building occupants.	√	√	√
7.16		The installation of a fire sprinkler system is either a pre-action or flooded system for areas excluding IT, power and mechanical rooms.	√	√	√
7.17		Manual systems, including manual pull stations and portable fire extinguishers are appropriately positioned throughout the data center.	√	√	√
7.18		Fire suppression systems are securely and properly mounted.	√	√	√
8.	**Security Standards**				
8.1	Door Security	Door access control is maintained 24/7.	√	√	√
8.2		An electronic access control system is in place.	√	√	√
8.3		Electronic access control system is implemented with multi-factor authentication for critical and mission - critical data centers (Tier III and IV).	√	√	x
8.4		The electronic access control system has the capability to	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		record access to all secure data center areas and retains those logs for a minimum of one year.			
8.5		Enforcement of strict policies and sign in/out logs are mandatory.	√	√	√
8.6		Review of procedures and sign in/out logs are done on a regular basis.	√	√	√
8.7		Secured doors are fail open in a fire emergency.	√	√	√
8.8	Video Surveillance	CCTV cameras cover all the area in the Data center for monitoring real time movements within the Data center.	√	√	√
8.9		Local and remote surveillance of secured and public spaces is allowed.	√	√	√
8.10		Recording devices (tape or hard disk) are located in a secure area.	√	√	√
8.11		Review of the recordings a regular basis to ensure proper operation of the video security system.	√	√	√
8.12		All security recordings are saved for no less than 90 days	√	√	√
8.13	Granting Security Access	Data center locations have a visitor/non-essential staff access policy.	√	√	√
8.14		Access must only be granted to essential personnel.	√	√	√
8.15		Visitors are signed in and out and are supervised at all times.	√	√	√
8.16		Visitor logs are maintained for a minimum of one year.	√	√	√
8.17	Emergency Procedures	All sites maintain published emergency procedures including fire Evacuation Plan	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		and emergency contact information.			
8.18		It performs regular emergency procedures awareness, trainings and testing as per the institutional Business Continuity Plan (BCP).	√	√	√
8.19		Exit routes are clearly marked with illuminated or photoluminescent signage placed across the facility to ensure safe and efficient evacuation.	√	√	√
8.20	ICT Security	A public institution shall ensure that all data center infrastructure and operations comply with the e-Government Security Architecture Standards and Technical Guidelines (eGA/EXT/ISA/001).	√	√	√
9.	**Monitoring Standards**				
9.1		All data center systems and infrastructure are monitored regularly.	√	√	√
9.2		For critical and mission - critical data centers (Tier III and IV), monitoring system for all installed equipment are installed in one centralized panel at Data Center Control Room.	√	√	x
9.3		Sensing cables are installed along room perimeter, under the raised floor, as well as areas prone to water leakage	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		such as HVAC units and water pipes.			
9.4		Air conditioning systems are specifically designed for stringent environmental control with automatic monitoring and control of cooling, heating, humidification, dehumidification, and air filtration function.	√	√	√
9.5		Data Center Control Room is provided with a separate air conditioning system so that the air conditioning units can be switched off whenever needed.	√	√	√
9.6		Access to the Data Center Room is controlled using access control system limited to only staffs who are responsible for managing and operating the Data center infrastructure.	√	√	√
9.7		The Data Center asset database is in place and updated whenever changes occur.	√	√	√
10.	**Maintenance Standards**				
10.1	Preventive maintenance	Public institution shall ensure that all equipment undergo preventive maintenance quarterly or as per manufacturer requirements, whichever is more stringent.	√	√	√
10.2	Building	Check the condition of floors, ceilings, and walls including leakage or damage and carry out necessary repairs	√	√	√
10.2		Make sure that exits are clearly marked, with additional signage as needed.	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
10.3		Make sure that data center is free of trash or large items that could be a fire or tripping hazard.	√	√	√
10.4		Conduct routine pest inspections and treatments.	√	√	√
10.6	ICT Equipment	ICT hardware equipment i.e. servers, communication gear, and storage equipment are racked in appropriate locations as per plan.	√	√	√
10.7		There is no loose wire on or above the floor.	√	√	√
10.8		The asset management database is used to create a removal list of all hardware, power, and connections related to the server(s).	√	√	√
10.9		All equipment to be removed are powered down before removal.	√	√	√
10.10		All servers and components to be removed are labeled, inventoried, and properly bundled for delivery to owner or disposal.	√	√	√
10.11		Blanking panels are installed in the vacated rack space.	√	√	x
10.12	Documentation	A change request documenting additional or removal is completed and approved before work begins.	√	√	√
10.13		The Data Center asset database and all other records relating to the equipment are updated to reflect the change	√	√	√
10.14	Disposition	The disposition of the server after removal are documented before the process starts.	√	√	√
10.15		All components are inventoried and a list created for the history	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		file and turnover to client or for disposal.			
10.16		All Institution's asset removal/repurpose forms are completed.	√	√	√
10.17		All items are processed in accordance with the Public Finance (Management of Public Property) Regulations, 2024 and the Electronic and Postal Communication (Electronic Communications Equipment Standards and E-Waste Management) (Amendments) Regulations, 2024.	√	√	√
10.18	Electrical Infrastructure	All electrical system components are regularly inspected and carry out necessary repairs.	√	√	√
10.19		Backup generators are available and are in good working order.	√	√	√
10.20		Automatic Transfer Switches (ATS), Uninterrupted Power Supplies (UPS), and Power Distribution Units (PDU) are in good working order.	√	√	√
10.21		The PDU/Wall Breaker Panel map are updated.	√	√	√
10.22		All unused or decommissioned power, data circuits, management circuits, and fiber connections are reclaimed and removed.	√	√	√
10.23		All breakers are turned off during maintenance of electrical equipment.	√	√	√
10.25	Cooling Infrastructure	Check and confirm that Computer Room Air Conditioners (CRAC) or	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
		Computer Room Air Handlers (CRAH) and the overall HVAC system is efficiently functional regularly.			
10.26		Replaces filters based on operational hours, manufacturer guidance or pressure drop-readings.	√	√	√
10.27		Clean evaporator coils regularly and ensure proper air filtration upstream.	√	√	√
10.28		Regularly inspect and adjust belt tension to the manufacturers recommended specifications.	√	√	√
10.26	Security and Safety	Check the locks and the doors, make sure that they lock and unlock easily.	√	√	√
10.27		Test smoke and carbon monoxide detectors and change batteries at least twice a year.	√	√	√
10.28		Check that all lights (interior and exterior) are working, replacing bulbs as needed.	√	√	√
10.29		Regularly check the visitors' list and try to limit access to the data center as much as possible.	√	√	√
10.30		Check the surveillance system is in good working order.	√	√	√
10.31	Cleaning	Check the cleanliness condition of the data center facility.	√	√	√
10.32		Make sure that the data center hardware equipment and the facility itself is free of dust and contamination.	√	√	√
	Operation standard				

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
10.33	Service Level Agreements	Services within the data center shall be maintained with the minimum service availability of 99.741% (22 hours of downtime annually) for Server Room (Tier II).	x	x	√
		Services within the data center shall be maintained with the minimum service availability of 99.982% (1.6 hours of downtime annually) for Critical Data Centers (Tier III).	x	√	x
		Services within the data center shall be maintained with the minimum service availability of 99.995% (26.3 minutes of downtime annually) for Mission Critical Data Centers (Tier IV).	√	x	x
10.34		All components of the data center facility shall be periodically tested to ensure they function properly. Records for these reports shall be kept appropriately.	√	√	√
10.35	Operations management	establish a standard operating procedures for data center operations.	√	√	√
10.36		clearly define roles and responsibilities for data center personnel.	√	√	√
10.37	Incident management	establish process and procedures for incident management, disaster recovery and business continuity.	√	√	√

S/ No		Standard Requirements	Mission - Critical Data Center (Tier IV)	Critical Data Center (Tier III)	Server Room (Tier II)
10.38		Ensure it tests the incident management plan, disaster recovery plan and business continuity plan.	√	√	√
10.39	Capacity management	Ensure the data center has sufficient capacity across compute, power, cooling, storage, networking, white space, and management infrastructure to reliably meet current and future demands.	√	√	√
10.40		Prepare capacity analysis reports quarterly.	√	√	√