THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE, PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

e-GOVERNMENT AUTHORITY

Document Title

Data Center Standards for Public Institutions

Document Number

eGA/EXT/IRA/003

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Jabiri Kuwe Bakari	Director General		12/2020

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 a number of 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. Jabiri Kuwe Bakari

DIRECTOR GENERAL

Table of Contents

1. INTRODUCTION

1.1 Overview

e-Government Authority also known as "e-GA" is a Government institution established by the e-Government Act No. 10 of 2019, that is mandated to coordinate, oversee and promote e-Government initiatives as well as enforcing e-Government related Policies, Laws, Regulations, Standards and Guidelines in Public Institutions.

Data center is a dedicated space within a building, or a group of buildings where used to house critical applications and storage systems. A data center design is based on a network of computing and storage resources that enable the delivery of shared applications and data. The Government Data Centers can be categorized into three types according to their criticality which are non-mission critical data centers, moderate critical data centers and critical data centers.

i. **Non-mission Critical Data Centers**: 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 (AD, LDAP), file servers etc.

ii. **Moderate Critical Data Centers:** These are Data Center facilities that are meant to accommodate some of the major systems of an organization. The systems to be housed are moderate critical systems for running daily operations of an organization.

iii. **Critical Data Centers**: These are Data Center facilities that accommodate major systems which are running daily business operations of an organization and serving other external entities including other institutions and private entities.

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 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 in order to ensure compliance with relevant provisions of the e-Government law, but it is also for ensuring continuity of business operations. To this end therefore, the Authority has developed these standards in order 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

The ideal Government data center in which public institutions host their ICT systems should meet the following standards:

2.1 Site Selection Standards

2.1.1 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 and evaluation and a risk analysis.
ii. The site selection process includes a detailed analysis of all the costs associated with any particular location.

2.1.2 Hazards

Public institution shall ensure that: -

i. The choice of the location, civil works and other installations guard the data center against disasters that are within human control such as floods, lighting, earthquake, fire etc.
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, or levee failure.
vi. For new building locations, the suitability of the site is verified by current documents, recent geological records, or by appropriate analytical measures.
vii. When placing a data center in close proximity to a railroad, measurement of vibration and EMI at the site is conducted over the period of several days to aid in the assessment and mitigation requirements, if any required at the site.

2.1.3 Site Access and location

A public institution shall ensure that: -

i. The placement of the building is not close enough to the road that an adjacent road traffic accident could result in vehicular contact with the building fabric or any external component of the data center mechanical or

electrical systems and potential for resulting structural damage or the potential for fire.

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. For disaster backup sites, considers the issue of distance from the primary data center.

2.1.4 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. Overhead utility service to the facility is not used, especially if there is only one service entrance fee. Instead, provide underground utility service to the facility whenever possible.

v. When selecting a site, considers space for one or more backup and one or more emergency generators and their associated electrical utility and life safety circuit paths.

vi. A data center is located in area with easy sustainable connectivity to the access provider central offices.

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

viii. Backup water supply is provided for data centers.

2.2 Space Planning Standards

2.2.1 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 storage room so that boxed equipment, spare air filters, spare floor tiles, spare cables, spare equipment, spare media and spare paper can be stored outside the computer room.

2.2.2 Power Systems

A public institution shall ensure that: -

i. Proper grounding for both lighting protection and grid power.
ii. In data centers that employ access floor systems, 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.

2.2.3 Cooling Capacity

A public institution shall ensure that: -

i. There is adequate cooling equipment as well as raised floor or overhead cable tray for more flexible cooling.
ii. The cabinets and racks are arranged in an alternating pattern to create hot and cold aisle.
iii. 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.

2.2.4 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.

2.2.5 Data Center Supporting Spaces

i. A public institution shall ensure that where possible, support equipment such as HVAC, UPS battery backup and generators is located outside of the data center production floor.

2.3 Architectural Standards

2.3.1 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 are documented.
iii. Physical and logical designs are updated whenever changes occur.
iv. data center design are developed with associated specifications and Bill of Quantities (BoQ)
v. A data center has been designed to accommodate diverse hardware designs and requirements, and possibly equipment from different manufacturers.
vi. The area has been designed to limit and control access.
vii. A data center has a single point of entry and sufficient set back of building for perimeter security purposes.
viii. Data center components have redundant (N+1) capacity components such as uninterruptable power supply (UPS), cooling systems and auxiliary generators.

2.3.2 Construction Components

A public institution shall ensure that: -

i. The building structural system is made of steel or concrete or fabric materials. 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.

2.4 Mechanical Systems Standards

A public institution shall ensure that: -

i. It has installed multiple HVAC systems for redundancy as opposed to relying on a single centralized chiller.
ii. An ambient temperature within the data center is between 70- and 74-degrees F.
iii. A relative humidity of 45 percent to 50 percent is maintained within the data center. 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.
iv. Alternate aisles between cold-aisle and hot aisle facilitates a more-efficient temperature control.
v. It maintains a static pressure within the raised floor plenum of 5 percent greater than the data center raised-floor area.
vi. It selectively positions perforated tiles in the raised floor to direct chilled air into the rack area.
vii. It seals all penetrations in the raised floor to maintain a constant static pressure.
viii. It establishes a vapour barrier throughout the perimeter of the data center to minimize condensation. Use spot cooling or special rack enclosures for hot spots in the data center layout.

2.5 Electrical Systems Standards

2.5.1 Main and step-down transformers

A public institution shall ensure that a transformer: -

i. Has been located in a secure mechanical room.
ii. Facility has HVAC systems to support heat load and correct humidity levels for each unit.
iii. Is maintained by a qualified technician to factory standards and be supportable by extended factory warranty.

2.5.2 Main power control panel and PLC (Program Logic Control)

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

i. Are maintained by a qualified technician to factory standards.
ii. Are located in a secure mechanical room.

iii. Have HVAC systems to support heat load and correct humidity levels for each unit.
iv. Have surge suppression sufficient to prevent large surges from damaging panels and equipment supported by panel.

(b) A public institution shall ensure that PLC: -
i. Have password security.
ii. Have UPS support for power failure.

2.5.3 Backup batteries

A public institution shall ensure that backup batteries: -

i. Follow manufacture's recommendations for system to be of sufficient quality and capacity to ensure a long life thus limiting breaks in the battery strings.
ii. Are located in secure area with proper ventilation as required.
iii. Are installed and maintained by authorized technicians.
iv. Are approved for use in computer equipment UPS systems
v. Facilities are able to sustain the expected load capacity for at least 3-5 hours on total power blackout.

2.5.4 UPS systems

A public institution shall ensure that UPS systems

i. Are sized to meet current and future needs, with sufficient battery backup to allow for a controlled shutdown of primary servers.
ii. Are designed, installed and maintained by authorized electricians and technicians and housed in a secure location. UPS systems follow manufacturer's recommended maintenance schedule.
iii. Have bypass capability to allow for periodic maintenance.
iv. are designed in redundant to provide non disruption of services during maintenance

2.5.5 Generator management

A public institution shall ensure that: -

i. Generators are tested and run for at least one hour in every month.
ii. A full load test and switching test is conducted at least yearly.
iii. Maintenance logs are kept on all tests and reflect all maintenance performed.
iv. A Data centre is supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HAVC).
v. All maintenances are performed by a qualified technician to factory specifications.
vi. Generator Management includes remote alarm panel (enunciator panel).

2.5.6 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.

2.5.7 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. Cables are aligned to minimize air flow disruptions.

2.5.8 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, CRACs, cable pathway, and any raised floor systems.
iii. Ground resistance is < 1 Ohm.

2.6 Cabling Infrastructure Standards

2.6.1 Overhead delivery system cable layout

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

2.6.2 Fiber standards

A public institution shall ensure that: -

i. Fiber installation uses 50-micron OM3/OM4 Laser optimized fiber.
ii. All fiber installations and copper data cables are labeled.
iii. Copper jumpers are of CAT6/CAT7 with Booted RJ45 connectors.

2.7 Fire Protection Standards

2.7.1 Fire Detection Standards

A public institution shall ensure that: -

i. Detectors include both heat and smoke-sensing devices (Proposed Very Early Smoke Detection System (VESDA)) and be interconnected with the fire suppression system, local alarms, and local or central monitoring stations.
ii. The detectors are positioned in relation to airflow patterns to ensure early detection of an imminent electrical fire.
iii. A separate fire alarm panel is deployed for Data Center area.
iv. The deployed fire alarm panel communicates the alarm signal to the master fire panel that monitors the entire premise.
v. The deployed fire alarm panel has the capability to send audio/visual signal at security area.

2.7.2 Fire Suppression Standards

A public institution shall ensure that: -

i. The installation of fire-rated walls is in accordance with the NFPA 75 standards.
ii. The installation of a sprinkler system is either a pre-action or flooded system.
iii. The use of a chemical or "clean agent" suppression system is the first line of defense. Manual systems, including manual pull stations and portable fire extinguishers that are positioned throughout the data center.

2.8 Security Standards

2.8.1 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 and log all access to secure data center areas.
iii. Access logs are maintained for a minimum of one year or longer as specified by site security policy.
iv. Enforcement of strict policies and sign in/out logs are mandatory.
v. Review of procedures and sign in/out logs are done on a regular basis.
vi. Secured doors are fail open in a fire emergency.

2.8.2 Video security

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. Recording is done on a regular basis to ensure proper operation of the video security system.
v. All security recordings are saved for no less than 30 days.

2.8.3 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 supervised at all times.
iv. Visitor logs are maintained for a minimum of one year or longer as specified by site security.

2.8.4 Emergency procedures

i. A public institution shall ensure that all sites maintain published emergency procedures that address:

- Emergency contact information
- Various and the respective site's planned responses
- Ongoing testing and staff awareness

2.8.5 Fire alarm and suppression systems

a) A public institution shall ensure that fire alarm and suppression systems: -

i. Are designed specifically for use in data centers.
ii. Comply with all state and local building codes.
iii. Are maintained by qualified technicians

b) A public institution shall ensure that suppression systems: -
i. Use chemicals that do not damage sensitive equipment.
ii. Does not pose harm to building occupants.
iii. Must be maintained by qualified technicians.

2.9 Monitoring Standards

A public institution shall ensure that: -

i. The monitoring system for all installed equipment are installed in one centralized panel at NOC Room.
ii. Sensing cable are installed along room perimeter especially along the glass windows and wall area, toilet adjacency area and under air condition units in order to sense liquid leakage.
iii. Air conditioning systems are specifically designed for stringent environmental control with automatic monitoring and control of cooling, heating, humidification, dehumidification, and air filtration function is installed.
iv. NOC area is provided with a separate air conditioning system so that the air conditioning units can be switched off whenever needed.
v. The equipment room is installed with fire rated door.
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.

2.10 Maintenance Standards

2.10.1 Building

A public institution shall: -

i. Check the condition of floors, ceilings and walls.
ii. Look for leakages or water damages in the ceilings.
iii. Make sure that exits are clearly marked, with additional signage as needed.
iv. Make sure that data center is free of trash or large items that could be a fire or tripping hazard.
v. Conduct routine pest inspections and treatments.

2.10.2 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. Blanking panels are installed in the vacated rack space.
vi. All servers and components are labeled, inventoried, and properly bundled for delivery to owner or eWaste.

2.10.3 Documentation

A public institution shall ensure that: -

i. A change request documenting removal is completed and approved before work begins.
ii. The asset database and all other records relating to this server are updated to reflect the change.
iii. If a unit is to go to eWaste, all inventory removal and eWaste forms are completed.

2.10.4 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 eWaste service.
iii. All Institution's asset removal/repurpose forms are completed.

iv. All items are processed using eWaste procedures for the disposal of electronic equipment.

2.10.5 Electrical Infrastructure

A public institution shall ensure that: -

i. All electrical system components are regularly inspected.
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) and their state of working condition are checked
iv. The PDU (Power Distribution Unit)/Wall Breaker Panel map are updated.
v. All power, data circuits, management circuits, and fiber connections are reclaimed and removed.
vi. All breakers are turned off.

2.10.6 Cooling Infrastructure

i. A public institution shall check and confirm that Computer Room Air Conditioners (CRAC) or Computer Room Air Handlers (CRAH) and the overall HVAC system is efficiently functional.

2.10.7 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 once 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.

2.10.8 Cleaning

A public institution shall: -

i. Check the cleanliness condition of the data center facility (ies).

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

2.10.9 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 Non-mission Critical Data Centers.
   b. 99.886% (10 hours of downtime annually) for Moderate Critical Data Centers.
   c. 99.982% (1.6 hours of downtime annually) for Critical Data Centers.

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

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

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

This document shall be:

3.1 Effective upon being signed by the Director General on its first page.
3.2 Subjected to review at least once every three years or whenever necessary changes are needed.
3.3 Consistently complied with, any exceptions to its application must duly be authorized by the Director General.

4. GLOSSARY AND ACRONYMS

4.1 Glossary

None

4.2 Acronyms

Abbreviation	Explanation

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
HAVC	Heat, Air Ventilation and Cooling
ICT	Information and Communication Technology
LDAP	Light Weight Directory Access Protocol
NOC	Network Operation Center
PLC	Program Logic Control
PDU	Power Distribution Unity
UPS	Uninterruptible Power Unity

5. RELATED DOCUMENTS

5.1. e-Government Infrastructure Architecture Standards and Technical guidelines (eGA/EXT/IRA/001).
5.2. e-Government Guideline (PO-PSM, 2017).
5.3. Telecommunication infrastructure standard for data centers (TIA-942)
5.4. Information Technology – Data Center Facilities and Infrastructure (ISO/IEC TS 22237).
5.5. [IEEE STD-- 802.11-2012].
5.6. [ANSI/TIA-568-C.3-1].
5.7. ISO/IEC 11801:2002/Amd 2:2010

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	e-GA	Creation of Document	December 2020

APPENDIX

Appendix I: Standards requirements for different Government Data Centers

S/ No		Standard Requirements	Critical Data Center	Moderate Critical Data Center	Non mission Critical Data Center
1.		**Site Selection Standards**			
1.1.	Site Evaluation	The suitability of a site shall be determined by a site survey and evaluation and a risk analysis.	√	√	√
1.2		If the data center is moving into an existing building, Public Institution should determine if the building is up to current code and industry standards.	√	√	√
1.3		The site selection process should include a detailed analysis of all the costs associated with any particular location.	√	√	√
1.4	Hazards	The choice of the location, civil works and other installation shall guard the data center against disasters that are within human control such as floods, lighting, earthquake, fire etc.	√	√	√
1.5		Seismically active areas should be avoided whenever possible.	√	√	√
1.6		Data center should be located outside the immediate risk area of an active volcano.	√	√	√
1.7		Data center should not be placed on the edge of urban development or near protected natural areas.	√	√	√
1.8		The site should be free of flood risk from river flood plain proximity, tidal basin proximity, dam failure, tsunami, or levee failure.	√	√	√

1.9		For new building locations, the suitability of the site should be verified by current documents, recent geological records, or by appropriate analytical measures.	√	√	x
1.10		When placing a data center in close proximity to a railroad, measurement of vibration and EMI at the site should be conducted over the period of several days to aid in the assessment and mitigation requirements, if any required at the site.	√	√	√
1.11	Site Access and location	The site should allow the placement of the building so that it is not close enough to the road that an adjacent road traffic accident could result in vehicular contact with the building fabric or any external component of the data center mechanical or electrical systems and potential for resulting structural damage or the potential for fire.	√	√	√
1.12		The data center should be 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.	√	√	√
1.13		For disaster backup sites, consider the issue of distance from the primary data center.	√	√	√
1.14	Utility Services	Adequate electrical utility capacity to the site shall be provided to meet both current and projected needs of the entire site.	√	√	√

1.15		Consider using multiple electrical utility circuits, each with enough capacity to handle the entire site requirements.	√	√	√
1.16		Data center should be 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
1.17		Overhead utility service to the facility is not recommended, especially if there is only one service entrance feed. Instead, provide underground utility service to the facility whenever possible.	√	√	√
1.18		When selecting a site, consider space for one or more backup and one or more backup and one or more emergency generators and their associated electrical utility and life safety circuit paths.	√	√	x
1.19		Data center should be located in area with easy sustainable connectivity to the access provider central offices.	√	√	√
1.20		Provide adequate water delivery to the site to meet the requirements of the data center.	√	√	√
1.21		Backup water supply shall be provided for data centers.	√	√	√
2.		**Space Planning Standards**			
2.1	Facility Capacity	The space around the data center must be considered for future growth and planned easy annexation.	√	√	√

2.2		Adequate space must be provided within and between racks, the cabinet and the pathways for better cable management, bend radius protection and access.	√	√	√
2.3		The data center should have an adequately sized storage room so that boxed equipment, spare air filters, spare floor tiles, spare cables, spare equipment, spare media and spare paper can be stored outside the computer room.	√	√	√
2.4	Power Systems	Public institution shall ensure proper grounding for both lighting protection and grid power.	√	√	√
2.5		In data centers that employ access floor systems, adequate separation of power and telecommunications cabling should be accommodated through allocating separate aisles for power and telecommunications cabling in the main aisles.	√	√	x
2.6		Vertical separation shall be 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 should be coordinated with architects, mechanical engineers and electrical engineers that are designing lighting, plumbing, air ducts, power and fire protection systems.	√	√	√
2.8	Cooling Capacity	There shall be adequate cooling equipment as well as	√	x	x

		raised floor or overhead cable tray for more flexible cooling.			
2.9		The cabinets and racks shall be arranged in an alternating pattern to create hot and cold aisle.	√	√	√
2.10		The air conditioning system shall be designed to provide the design temperature and humidity conditions recommended by the manufacturers of the services to be installed within the data center.	√	√	√
2.11	Security	Truck loading docks shall be provided as required to handle anticipated deliveries, and shall be provided with a level of security similar to the other building entrances.	√	√	√
2.12		Locate the data center inside the existing building so there are no exterior windows or doors.	√	√	√
2.13		In situations where you must share data center space with other institutions, an effective means of segregating the space should be considered.	√	√	x
2.14	Data Center Supporting Spaces	Where possible, support equipment such as HVAC, UPS battery backup and generators should be located outside of the data center production floor.	√	√	x
3.		**Architectural Standards**			
3.1	General Design Concepts	A data center shall be designed with plenty of flexible white space that can accommodate future racks or cabinets.	√	√	√
3.2		The space around the data center must be considered for	√	√	√

		future growth and planned easy annexation.			
3.3		Public institution shall ensure that the 'as built' physical and logical designs of the data center are documented.	√	√	√
3.4		Physical and logical designs shall be updated whenever changes occur.	√	√	√
3.5		Public institution shall develop data center design with associated specifications and Bill of Quantities (BoQ)	√	√	√
3.6		The data center must be designed to accommodate diverse hardware designs and requirements, and possibly equipment from different manufacturers.	√	√	√
3.7		Design the area to limit and control access.	√	√	√
3.8		Single point of entry and sufficient set back of building for perimeter security purposes.	√	√	√
3.9		The data center components should have redundant (N+1) capacity components such as uninterruptable power supply (UPS), cooling systems and auxiliary generators.	√	√	x
3.10	Construction Components	The building structural system should be either steel or concrete or fabricated. At a minimum, the building frame should be designed to withstand wind loads in accordance with applicable building codes for relevant institutions charged with building approvals.	√	√	x
3.11		Floors, walls and ceiling shall be sealed, painted or	√	√	√

		constructed of a material to minimize dust.			
3.12		Walls, floors and ceilings shall be light in colour to enhance room lighting.	√	√	√
4.		**Mechanical Systems Standards**			
4.1		Strive for redundancy in the HVAC system by installing multiple units.	√	√	x
4.2		Ensure an ambient temperature between 70- and 74-degrees F.	√	√	√
4.3		Maintain a relative humidity of 45 percent to 50 percent and strive for redundant systems by installing multiple HVAC units (as opposed to relying on a single centralized chiller). Designing the airflow 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
4.4		Alternate aisles between cold-aisle and hot aisle facilitates a more-efficient temperature control.	√	√	x
4.5		Maintain a static pressure within the raised floor plenum of 5 percent greater than the data center raised-floor area.	√	x	x
4.6		Selectively position perforated tiles in the raised floor to direct chilled air into the rack area.	√	√	x
4.7		Be sure to seal all penetrations in the raised floor to maintain a constant static pressure.	√	x	x

4.8		Establish a vapour barrier throughout the perimeter of the data center to minimize condensation. Use spot cooling or special rack enclosures for hot spots in the data center layout.	√	x	x
5.		**Electrical Systems Standards**			
5.1	Main and step down transformers	Must be located in a secure mechanical room.	√	√	x
5.2		Must have HVAC systems to support heat load and correct humidity levels for each unit.	√	√	x
5.3		Must be maintained by a qualified technician to factory standards and be supportable by extended factory warranty.	√	√	x
5.4	Main power control panel and PLC	PLC must be maintained by a qualified technician to factory standards.	√	x	x
5.5		PLC must be located in a secure mechanical room.	√	x	x
5.6		Must have HVAC systems to support heat load and correct humidity levels for each unit.	√	√	x
5.7		Must have surge suppression sufficient to prevent large surges from damaging panels and equipment supported by panel.	√	x	x
5.8		PLC must have password security.	√	x	x
5.9		PLC must have UPS support for power failure.	√	x	x
5.10	Backup Batteries	Must follow manufacture's recommendations for system to be of sufficient quality and capacity to ensure a long life thus limiting breaks in the battery strings.	√	√	√
5.11		Must be located in secure area with proper ventilation as required.	√	√	√

5.12		Must be installed and maintained by authorized technicians.	√	√	√
5.13		Must be approved for use in computer equipment UPS systems	√	√	√
5.14		The power backup facility should be able to sustain the expected load capacity for at least 3-5 hours on total power blackout.	√	√	x
5.15	UPS Systems	UPS systems in the data center must be sized to meet current and future needs, with sufficient battery backup to allow for a controlled shutdown of primary servers.	√	√	√
5.16		UPS systems must be designed, installed and maintained by authorized electricians and technicians and housed in a secure location. UPS systems follow manufacturer's recommended maintenance schedule.	√	√	x
5.17		UPS systems must have bypass capability to allow for periodic maintenance.	√	√	√
5.18		UPS system must be designed in redundant to provide non disruption of services during maintenance	√	√	√
5.19	Generator Management	Generator must be start tested and run for at least one hour once a month.	√	√	x
5.20		A full load test and switching test must be conducted at least yearly.	√	√	x
5.21		Maintenance logs must be kept on all tests and reflect all maintenance performed.	√	√	√

5.22		The Data centre should be supported by a dedicated power generator enough to power the IT load capacity and the supporting components (HAVC).	√	√	x
5.23		All maintenance must be performed by a qualified technician to factory specifications.	√	√	x
5.24		Management must include remote alarm panel (enunciator panel).	√	x	x
5.25	Power strips	Must be sized to meet the power requirements of the cabinet in which they are installed.	√	√	√
5.26		Power receptacles for power strips must be installed by qualified electricians.	√	√	x
5.27	Power cable layout	Equipment power cables should be the minimum required length and slack/strain management must be employed.	√	√	√
5.28		Cables must be arraigned to minimize air flow disruptions.	√	√	√
5.29	Grounding Systems	All data center equipment must be grounded in compliance with state and local codes.	√	√	√
5.30		Data center equipment grounds must be independent of all other building grounds (such as lightning protection systems).	√	√	√
5.31		All metal objects must be bonded to ground including cabinets, racks, PDUs, CRACs, cable pathway, and any raised floor systems.	√	√	x
5.32		Ground resistance should be < 1 Ohm.	√	√	√
6.		**Cabling Infrastructure Standards**			

6.1	Overhead delivery system cable layout	The data room must have a system to support overhead delivery of data connections to the equipment cabinets.	√	√	√
6.2	Fiber Standards	Fiber installation must use 50 micron OM3/OM4 Laser optimized fiber.	√	√	x
6.3		All fiber installations must be labeled.	√	√	√
6.4		Copper jumpers must be CAT6/CAT7 with Booted RJ45 connectors.	√	√	√
6.5		All copper data cables must be labeled.	√	√	√
6.6	Grounding	All cabinets and cable delivery pathways must be grounded.	√	√	√
7.		**Fire Protection Standards**			
7.1	Fire Detection Standards	Detectors should include both heat and smoke-sensing devices (Proposed Very Early Smoke Detection System (VESDA)) and be interconnected with the fire suppression system, local alarms, and local or central monitoring stations.	√	√	√
7.2		The detectors should be positioned in relation to airflow patterns to ensure early detection of an imminent electrical fire.	√	√	√
7.3		A separate fire alarm panel should be deployed for Data Center area.	√	√	√
7.4		The Data Center area fire alarm panel should communicate the alarm signal to the master fire panel that monitors the entire premise.	√	√	√
7.5		The Data Center fire alarm panel should have the capability to send	√	x	x

		audio/visual signal at security area.			
7.6	Fire Suppression Standards	The installation of fire-rated walls in accordance with the standard.	√	√	√
7.7		The installation of a sprinkler system — either a pre-action or flooded system.	√	√	x
7.8		The use of a chemical or "clean agent" suppression system as the first line of defense. Manual systems, including manual pull stations and portable fire extinguishers that are positioned throughout the data center.	√	√	x
8.		**Security Standards**			
8.1	Door Security	Door access control must be maintained 24/7.	√	√	√
8.2		An electronic access control system should be in place and log all access to secure data center areas.	√	√	√
8.3		Access logs should be maintained for a minimum of one year or longer as specified by site security policy.	√	√	x
8.4		Enforcement of strict policies and sign in/out logs is mandatory.	√	√	√
8.5		Review of procedures and sign in/out logs must be done on a regular basis.	√	√	√
8.6		Secured doors must fail open in a fire emergency.	√	√	√
8.7	Video Security	CCTV camera should cover all the area in the Data center for monitoring real time movements within the Data center.	√	√	x
8.8		Allows for local and remote surveillance of secured and public spaces.	√	√	x

8.9		Recording device (tape or hard disk) must be located in a secure area.	√	√	x
8.10		Recording must be done on a regular basis to ensure proper operation of the video security system.	√	√	x
8.11		All security recordings must be saved for no less than 30 days.	√	√	x
8.12	Granting Security Access	Data center locations must have a visitor/non-essential staff access policy.	√	√	√
8.13		Access must only be granted to essential personnel.	√	√	√
8.14		Visitors must be signed in and out and be supervised at all times.	√	√	√
8.15		Visitor logs should be maintained for a minimum of one year or longer as specified by site security.	√	√	x
8.16	Emergency Procedures	All sites must maintain published emergency procedures that address: – Emergency contact information – Various and the respective site's planned responses – Ongoing testing and staff awareness	√	√	√
8.17	Fire Alarm and Suppression Systems	Must be designed specifically for use in data centers.	√	√	√
8.18		Must comply with all state and local building codes.	√	√	√

8.19		Suppression systems must use chemicals that do not damage sensitive equipment.	√	√	√
8.20		Suppression systems must not pose harm to building occupants.	√	√	√
8.21		Must be maintained by qualified technicians.	√	√	√
9.		**Monitoring Standards**			
9.1		The monitoring system for all installed equipment should be installed in one centralized panel at NOC Room.	√	√	x
9.2		Sensing cable should be installed along room perimeter especially along the glass windows and wall area, toilet adjacency area and under air condition units in order to sense liquid leakage.	√	√	x
9.3		Air conditioning systems specifically designed for stringent environmental control with automatic monitoring and control of cooling, heating, humidification, dehumidification, and air filtration function should be installed.	√	√	x
9.4		CCTV camera should cover all the area in the Data center for monitoring real time movements within the Data center.	√	√	x
9.5		NOC area should be provided with a separate air conditioning system so that the air conditioning units can be switched off whenever needed.	√	√	x
9.6		The equipment room should be installed with fire rated door.	√	√	√

9.7		Access to the Data center room should be controlled using access control system limited to only staffs who are responsible for managing and operating the Data center infrastructure.	√	√	√
10.		**Maintenance Standards**			
10.1	Building	Check the condition of floors, ceilings and walls.	√	√	√
10.2		Look for leaks or water damage in the ceilings.	√	√	√
10.3		Make sure that exits are clearly marked, with additional signage as needed.	√	√	√
10.4		Make sure data center is free of trash or large items that could be a fire or tripping hazard.	√	√	√
10.5		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		Make sure there are no loose wire on or above the floor.	√	√	√
10.8		The asset management database must be used to create a removal list of all hardware, power, and connections related to the server(s).	√	√	√
10.9		All equipment to be removed must be powered down before removal.	√	√	√
10.10		Blanking panels must be installed in the vacated rack space.	√	√	√
10.11		All servers and components must be labeled, inventoried, and properly bundled for delivery to owner or eWaste.	√	√	x

10.12	Documentation	A change request documenting removal must be completed and approved before work begins.	√	√	√
10.13		The asset database and all other records relating to this server must be updated to reflect the change.	√	√	√
10.14		If this unit will go to eWaste, all inventory removal and eWaste forms must be completed.	√	√	x
10.15	Disposition	The disposition of the server after removal must be documented before the process starts.	√	√	√
10.16		All components must be inventoried and a list created for the history file and turnover to client or eWaste service.	√	√	x
10.17		All Institution's asset removal/repurpose forms must be completed.	√	√	√
10.18		All items will be processed using eWaste procedures for the disposal of electronic equipment.	√	√	x
10.19	Electrical Infrastructure	All electrical system components should be regularly inspected.	√	√	√
10.20		Make sure that Backup generators are available and are in good working order.	√	√	x
10.21		Check Automatic Transfer Switches (ATS), Uninterrupted Power Supplies (UPS), and Power Distribution Units (PDU) and their state of working condition.	√	√	√
10.22		The PDU (Power Distribution Unit)/Wall Breaker Panel map must be updated.	√	√	√

10.23		All power, data circuits, management circuits, and fiber connections must be reclaimed and removed.	√	√	√
10.24		All breakers must be turned off.	√	√	√
10.25	Cooling Infrastructure	Check and confirm that Computer Room Air Conditioners (CRAC) or Computer Room Air Handlers (CRAH) and the overall HVAC system is efficiently functional.	√	√	x
10.26	Security and Safety	Check the locks the door, make sure they lock and unlock easily.	√	√	√
10.27		Test smoke and carbon monoxide detectors and change batteries at least once 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	Cleaning	Check the cleanliness condition of the data center facility.	√	√	√
10.31		Make sure that the data center hardware equipment and the facility itself is free of dust and contamination.	√	√	√
10.32	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 Non-mission Critical Data Center.	x	x	√
		Services within the data center shall be maintained	x	√	x

		with the minimum service availability of 99.886% (10 hours of downtime annually) for Moderate Critical Data Center.			
		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 Center.	√	x	x
10.31		All components of the data center facility shall be periodically tested to ensure they function properly. Records for these reports shall be kept appropriately.	√	√	√