GOVERNMENT ICT STANDARDS

Data Centre Standard

ICTA.2.002:2019

Second Edition 2019

REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICTA Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

ICT AUTHORITY (ICTA)

Head Office: P.O. Box 27150, Nairobi-00100, Tel.: (+254 202) 211 960/61
E-Mail: standards@ict.go.ke, Web:http://standards.icta.go.ke

DOCUMENT CONTROL

Document Name:	Government Data Centre Standard
Prepared by:	Government Data Centre Standard Technical Committee
Edition:	Second Edition
Approved by:	Board of Directors
Date Approved:	13th January 2020
Effective Date:	1st February 2020
Next Review Date:	After 3 years

Contents

FOREWORD

The ICT Authority has the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology including Systems, Infrastructure, Processes, Human Resources and Technology for the public service. The overall purpose of this mandate is to ensure coherent and unified approach to acquisition, deployment, management and operation of ICTs across the public service in order to achieve secure, efficient, flexible, integrated and cost effective deployment and use of ICTs.

To achieve this mandate, the Authority established a standards committee to identify the relevant standard domains and oversee the standards development process. The committee consulted and researched broadly among subject matter experts to ensure conformity to acceptable international and national industry best practices as well as relevance to the Kenyan public service. The committee eventually adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In an engagement founded on a memorandum of understanding KEBS, participated in the development of these Standards and gave invaluable advice and guidance.

For example, the Data Centre Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines which are, in turn, based on the international best practices by standards development organizations including ISO.

The Authority's Directorate of Programmes and Standards has the oversight role and responsibility for management, enforcement and review of this standard. The Directorate shall carry out quarterly audits in all the Ministries, Counties, and Agencies (MCA) to determine compliance to this Standard. The Authority shall issue a certificate for compliance to agencies upon inspection and assessment of the level of compliance to the standard. For non-compliant agencies, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the Standards Review Board who shall advise and make recommendations to remedy the shortfall.

The ICT Authority management, conscious of the central and core role that standards play in public service integration, fostering shared services and increasing value in ICT investments, shall prioritize the adoption of this standard by all Government agencies. The Authority therefore encourages agencies to adhere to this standard in order to obtain value from their ICT investments.

Dr. Katherine W. Getao, EBS

Chief Executive Officer

ICT Authority

1.0 INTRODUCTION

The data center is home to the computational power, storage, and applications necessary to support an enterprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered. All government data centres are expected to provide enough capacity to support all the necessary IT functions of government. The principal goals in data centre design are flexibility and scalability, which involve site location, building selection, floor layout, electrical system design, mechanical design and modularity. The advent of new technologies, such as blade servers, that require substantial incremental power and cooling capacity; the pressure to consolidate multiple data centres into fewer locations; the need for incremental space; changes in operational procedures; and potential changes in safety and security regulations converge to impose constant facilities changes on the modern data centre. Data centre standards will look at the best possible ways of setting up a data centre for government use. This will involve the design of the data centre, arrangement of equipment, operating conditions, security procedures and practices as well as any other requirement that would go into coming up with a modern and efficiently operational data centre. The data centre infrastructure should therefore be robust enough to support large amounts of data flow that government handles and efficient enough to ensure continues service availability. The conditions in the data centre should also be ideal to support the optimal operations of its infrastructure while the management of the data centre should also be easily adaptable to the current and future government operations. In order to design, build and operate an efficient data center, there is need to have guidelines that offer the industry acceptable specifications. This section outlines these guidelines that will be adopted by the government to ensure that it reaps the maximum benefits associated with it data centre operations.

2.0 SCOPE

These guidelines are grouped into the following domains:
- Design and Planning (physical location)
- Planning Layout
- Cabling infrastructure
- Environment (Cooling, power and lightning, fire detection and suppression)
- Physical Security
- Data center monitoring
- Maintenance and SLAs

Applications

This standard will be applicable to the following:
- ❖ Central Government of Kenya
- ❖ County Governments
- ❖ Constitutional Commissions
- ❖ State Corporations

3.0 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards.

- ANSI/TIA-569-c
- ANSI/TIA-568-c.1
- ISO/IEC 60793
- IEEE, 802.3
- IEEE, 802.1
- IETF RFC 3457, 2709, 1518, 1918
- [ANSI/TIA-568-c.2]
- [ANSI/TIA-568-B.2.1]
- [IEEE 802.3af]
- [ANSI/TIA-568-C.3-1]
- [(ITU-T) Series G.652]
- [IEEE STD-- 802.3-2008]
- [IEEE 802.3an 2006]
- [TIA/EIA 568-B.3]
- [ISO/IEC 11801:2002]
- [ANSI/TIA-568-c.3]
- [IEEE STD-- 802.11-2012]
- [IEEE STD 802.11-2011]
- [IEEE 802.1x]
- [IEEE 802.11i, g]
- [ISO/IEC 17799:2005(E)]
- [IEEE 802.1Q]
- [ISO/IEC 17799:2000]
- [IEEE STD-- 802.3-2008]
- [IEEE 802.3an 2006]
- IEC 62305-4

4.0 DEFINITIONS

For the purposes of this ICTA Standard the following definitions, abbreviations and symbols apply:

4.1 Anti-tailgating
Anti-tailgating refers to an access control for restricting an unauthorized person from gaining access through a turnstile or gate after an authorized person has already gained access.

4.2 Backbone Cable
Is the inter-building and intra-building cable connections in structured cabling between entrance facilities, equipment rooms and telecommunications closets. Backbone cabling consists of the transmission media, main and intermediate cross-connects and terminations at these locations.

4.3 CCTV
CCTV refers to closed-circuit television, or the use of video cameras to transmit images to a specific limited number of televisions on the same network or circuit.

4.4 Cyber Crime
Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

4.5 Data Center
A large group of networked computer servers typically used by organizations for the remote storage, processing, or distribution of large amounts of data.

4.6 Equipment Distribution Area
Is used in large computer rooms that need additional configuration flexibility between the HDA and equipment. The ZDA houses only passive equipment.

4.7 Horizontal Distribution Area (HDA)
Is the space where the horizontal cross-connect resides. It is the main transition point between backbone and horizontal cabling and houses the LAN, SAN and KVM switches that connect to the active equipment (servers, mainframes, storage devices).

4.8 Hot and Cold aisle
Hot aisle/cold aisle refers to a layout design especially for data warehouses whose purpose is to manage air flow in data centers, consequently lowering the energy, cooling and management cost inside data centers

4.9 Intruder Detection System
Software application that monitors a network or systems for malicious activity or policy Violations.

4.10 Main Distribution Area (MDA)
Is the hub of the cabling system. It includes the cross connect and the horizontal cross-connects if the equipment they serve is nearby. It holds the core routers and the core LAN/SAN switches.

4.11 Multimode Fiber
Multi-mode fiber is a type of optical fiber designed to carry multiple light rays or modes simultaneously, each at a marginally different reflection angle inside the optical fiber core.

4.12 Multi-tenant building
 Refers to a facility in which organizations can rent space to host their data. Businesses can rent to meet varying needs, from a server rack to a complete purpose-built module.

4.13 Power Distribution Units
A power distribution unit (PDU) is a type of electrical component that distributes and manages electricity supply to computers, servers and networking devices within a data center environment.

4.14 Rack
A rack is a type of physical steel and electronic framework that is designed to house servers, networking devices, cables and other data center computing equipment. This physical structure provides equipment placement and orchestration within a data center facility.

4.15 Whitespace
In data center, it refers to the area where IT equipment are placed.

4.16 Zone Distribution Area (ZDA)
Is used in large computer rooms that need additional configuration flexibility between the HDA and equipment. The ZDA houses only passive equipment.

5.0 ABBREVIATIONS

ANCI   American National Standards Institute
BoQ   Bill of Quantites
CCTV   Closed Circuit Television
EDA   Equipment Distribution Area
GEA   Government Enterprise Architecture
HDA   Horizontal Distribution Area
HVAC   Heating, Ventilation, and Air conditioning
IEC   International Electrotechnical Commission
IEEE   Institute of Electrical and Electronics Engineers
IETF   Internet Engineering Task Force
ISO   International Organization for Standardization
ISPs   International Ship and Port Facility Security
ITU   International Telecommunication Union
MCDAS Ministry, Counties, Departments and Agencies
MDA   Main Distribution Area
NFPA   National Fire Protection Association
PDU   Power Distribution Units

SLA   Service-level agreement
TIA   Telecommunications Industry Association

UPS   Uninterruptible Power Supply
ZDA   Zone Distribution Area

6.0 DATA CENTER DESIGN AND PLANNING

6.1.1   MCDA shall carry out site surveys to ensure a data center design is in line with the tiered reliabilities.

6.1.2   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, lightning, earthquake, fire etc.

6.1.3   MCDA shall ensure proper grounding forboth lightning protection and grid power. Type 1+2 surge arrestors should be installed to protect the data center from lightning(as guided by IEC 62305-4).

6.1.4   MCDA shall develop a data center design with associated specifications and Bill of Quantites (BoQ)

6.1.5   MCDA shall ensure that relevant construction and equipment installation is done in line with the specifications and Bill of Quantites (BoQ)

6.1.6   Upon completion of the construction and equipment installation MCDA shall carry out the tests and the results formally documented.

6.1.7   MCDA shall ensure that the 'as built' physical and logical designs of the data centerare documented.

6.1.8   MCDA shall ensure that the data center project iscommissioned and a Completion Certificate issued.

6.1.9   Physical and logical designs shall be updated whenever changes occur.

6.1.10 MCDA shall ensure that the Data center is designed with flexible and adequate "white space" empty space that can accommodate future racks and cabinets. The space sorrounding the data center must also be considered for future expansion (the facility specifications should be in line with TIA-942 standard).

6.1.11 MCDA shall ensure that the data center includes the following key functional areas (as guided by TIA-942); an Entrance Room, Main Distribution Area (MDA), Horizontal Distribution Area (HDA), Zone Distribution Area (ZDA) and Equipment Distribution Area (EDA) as minimum functional areas. The data center should also have a staging area for unpacking and possibly for testing new equipment before deploying them in the computer room.

6.1.12 MCDA shall consider arrangements for failover / backup facility for business continuity management.

7.0 PLANNING LAYOUT

7.1   Whitespace

7.1.1   A data center shall be designed with plenty of flexible white space that can accommodate future racks or cabinets.

7.1.2   The space around the data center must be considered for future growth and planned for easy annexation.

7.1.3   MCDA shall ensure that there is adequate space between the racks/cabinets. The layout should have both hot and cold aisleswith a minimumof 1.2 meter for the cold aisle and a minimum of 1.0 meters on the hot aisle.

7.1.4   Wrist strap ports shall be attached to the rack by a means that ensures electrical continuity to ground for static discharge.

7.1.5   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 the applicable building codes for the relevant institutions charged with building approvals.

7.1.6   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.

7.1.7   Every data center shall fall under any of the tiers as per TIA-942 Standard that will be determined from Appendix 1.

7.2   Cooling

7.2.1   There shall be adequate cooling equipment aswell as raised floor/overhead cable tray for more flexible cooling.

7.2.2   The cabinets and racks shall be arranged in an alternating pattern to create hot and cold aisle.

7.2.3   The air-conditioning system shall be designed to provide the design temperature and humidity conditions recommended by the manufacturers of the servers to be installed within the data center

7.2.4   A 24/7/365 dedicated HVAC system with automatic dampers and connected to a backup generator.

7.2.5   MCDA shall ensure when building new offices/identifying occupation of a new premises that considerations are made for a provision of a floor that meets the data center required minimum height (18 inches).The recommended rack and cabinet height shall be 2.4 m (8 ft). Racks and cabinets shall preferably be no taller than 2.1 m (7 ft) for easier access to the equipment or connecting hardware installed at the top.

7.3   Power

7.3.1   Power requirements shall be based on the desired reliability tier as per tiered reliability standard- (See Appendix 1) and may include two or more power feeds from the utility, UPS, Multiple circuits to systems and equipment, and on-site generators.

7.3.2   Power requirements shall be estimated for all the existing devices and for devices anticipated in the future.

7.3.3   Power estimation must be made to accommodate required redundancy and future growth.

7.3.4   Every data center shall be supported by generator(s) and UPS System(s) and shall be designed to supply the harmonic current imposed by the UPS system or computer equipment loads. The UPS batteries should be able to support the computer systems for at least 8 hrs.

7.3.5   Data Centre shall have a Power Distribution Units (PDUs) for distribution to critical electronic equipment.

7.3.6   MCDA are encouraged to consider the use of green power to cut on cost of power consumption

7.3.7   Data center shall at all times have fire detection, extinguisher and suppression systems.

7.4 Fire Detection and Suppression

7.4.1 The data center construction shall be separated from other occupancies by fire resistant rated construction (not less than an hour). Every opening in the fire resistant construction shall be protected to limit spread of fire and to restrict the movement of smoke from one side to the other.

7.4.2 Automatic detection material shall be installed to provide early fire warning and the equipment used shall be a listed smoke detection type system. The alarms and trouble signals of automatic detection or extinguishing system shall be arranged to annunciate in a constantly occupied location.

7.4.3 MCDA shall ensure that the IT personnel designated to man the facility are continually and thoroughly trained in the functioning of the alarm system, desired response to alarm condition, location of emergency equipment, tools and all available extinguishing equipment.

7.4.4 MCDA shall ensure that appropriate extractor fans are installed to extract any gas discharge / leakage.

7.4.5 The fire protection systems and hand-held fire extinguishers shall comply with NFPA-75.

8.0   CABLING INFRASTRUCTURE

8.1 Cabling

8.1.1 Data centers shall use a minimum laser-optimized 50 microns multimode fiber for backbone cabling and with minimum 24 cores backbone cable.

8.1.2 Data centers shall use the highest capacity horizontal cabling media available as recommended by the current IEEE 802.3 standards to reduce the need for re-cabling in the future

8.1.3 A data center shall be designed with separate racks and pathways for each media type. The power and communication cables shall be separated on different pathways or separated by a physical barrier.

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

8.1.5 A labeling scheme for all racks, power, cabinets, patch panels, patch cords and cables must be maintained.

8.1.6　Branch circuits in data centers shall be in watertight flexible metal conduit. Feeder circuits to power distribution units and panels shall be installed in solid metal conduit. If the feeder circuits are not in solid metal conduit, they should be in watertight flexible metal conduit.

8.1.7　In data centers that use overhead cable trays, the normal separation distances provided by standard practices provides adequate separation. As specified in ANSI/TIA-569-B, a minimum of 300 mm (12 in) access headroom between the top of a tray or runway and the bottom of the tray or runway above shall be provided and maintained.

8.1.8　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. Where this is not possible, horizontal and vertical separation of power and telecommunications cables shall be provided.

8.1.9　In addition, vertical separation shall be provided by placing the telecommunications cabling in cable trays or baskets as far above the power cables as possible, preferably with the top of the cable tray or basket 20 mm (0.75 in) below the bottom of the access floor tile; in the equipment cabinet aisles, allocate separate aisles for power and telecommunications cabling as maybe applicable.

8.1.10　Current alternate standard to raised floor

8.1.11　Cables shall not be left abandoned under the access floor or in overhead cable trays and shall be terminated on at least one end in the main distribution area or a horizontal distribution area, or removed.

8.1.12　Planning of 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. Lighting fixtures and sprinkler heads should be placed between cable trays, not directly above cable trays.

8.1.13　There should be full redundancy in the data center network; Use two or more ISPs and pairs of IT equipment.

9.0   ENVIRONMENT AND AMBIENCE

9.1   Physical

9.1.1   The room shall be protected from contaminants in accordance with ANSI/TIA-569-B.

9.1.2   The Building design shall guard against excessive computer room vibration.

9.1.3   Floors, walls and ceiling shall be sealed, painted or constructed of a material to minimize dust.

9.1.4   Walls, floors and ceilings shall be light in color to enhance room lighting. Floors shall have anti-static properties as per IEC 61000-4-2.

9.1.5   Sprinkler systems in computer rooms shall be pre-action systems, where risk of water ingress exists, a means of evacuating water from the space shall be provided (e.g. a floor drain). Any water and drain pipes that run through the room should be located away from and not directly above equipment in the room.

9.1.6   Equipment should be placed in cabinets and racks with "cold" air intake at the front of the cabinet or rack, and "hot" air exhaust out the back.

9.1.7   Blank panels should be installed in unused rack and cabinet spaces to improve the functioning of "hot" and "cold" aisles. Perforated access floor tiles should be located in the "cold" aisles rather than in the "hot" aisles to improve the functioning of the "hot" and "cold" isles.

9.1.8   A minimum of 1 m (3 ft.) of front clearance shall be provided for installation of equipment. A front clearance of 1.2 m (4 ft.) is preferable to accommodate deeper equipment. A minimum of 0.6 m (2 ft.) of rear clearance shall be provided for service access at the ear of racks and cabinets. A rear clearance of 1 m (3 ft.) is preferable. Some equipment may require service clearances of greater than 1 m (3 ft.) as may be guided by equipment manufacturer requirements.

9.1.9   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.

9.1.10 Access to the data Centre shall require protective gears/garments to minimize dust and other risks.

9.1.11 The data Centre building shall conform to all applicable national, state, and local codes.

9.1.12 Where the building is not dedicated to the data center, other tenant spaces should be non-industrial, International Building Code type 'B' offices, and non-intrusive to the data center. Avoid buildings with restaurants and cafeterias to minimize fire risk.

9.1.13   If the data center is to be on an upper floor of a multi-tenant building, then there shall be adequate shaft and conduit space for generator, security, telecommunications, and electrical conduits as well as supplemental HVAC, grounding conductors and cabling to antennas, as needed.

9.1.14   The building hosting the data Centre shall not be in the flight path of any nearby airports. The building shall be no closer than 0.8 km (½ mile) from a railroad or major interstate highway. The building shall not be within 0.4 km (¼ mile) of an airport, research lab, chemical plant, landfill, river, coastline, or dam as applicable. The building shall not be located adjacent to a foreign embassy the building shall not be located in high crime areas.

9.2   Cooling

9.2.1   There shall be adequate cooling equipment as well as raised floor system for more flexible cooling as may be appropriate.

9.2.2   The air-conditioning system shall be designed to provide temperature and humidity conditions recommended by equipment manufacturers. The temperature and humidity shall be controlled to provide continuous operating ranges for temperature and humidity.

9.2.3   There shall be a 24/7 dedicated HVAC system with automatic dampers and connected to a backup generator.

9.3   Power

9.3.1   Power requirements will be based on the desired reliability as per tiered reliability standard – Appendix 1.

9.3.2   The power system shall be supported by at least two standby generator system. Where batteries are used for backup, adequate ventilation and spill containment as required shall be provided.

10.0 PHYSICAL SECURITY

10.1   The perimeter of the site shall be protected by appropriate intruder detection system and monitored by visible or infrared Closed Circuit Television (CCTV) system. All common areas shall be monitored, including parking lots, loading docks, and building entrances.

10.2   Access to the site shall be secured by identification and authentication systems.

10.3   There shall be only one single point of entry. Consideration can be made for physical access control with anti-tailgating / anti-pass-back turn-style gate that permits only one person to pass at any one time after authentication.

10.4   The security of information at the data center should be in line with; information security standard, ISO 27001/2, and the computer misuse and cybercrime Act 2018

11.0 DATA CENTER MONITORING

11.1   MCDA shall ensure that monitoring system are installed to check the health status of all the active and computing devices.

11.2   MCDA shall install a monitoring tool to check on the data center environment i.e. temperature, humidity and power.

11.3   MCDA shall install a real time monitoring system to check the Physical security of the data center.

12.0 MAINTENANCE AND SLAS

12.1   All the components of the data center shall be tested periodically once the data center is in operation to ensure that they will continue to function properly. The records for the test shall be kept always.

12.2   Maintenance programs shall be identified to detect imminent or conditional failures for all data center equipment and service tags / maintenance schedule.

12.3   MCDA shall ensure Service Level Agreement (SLA) are maintained with a minimum of data center services availability of 99.99%.

APPENDIX I

Tiered Reliability Standard

Refer to the uptime Institute standard

Tier 1 = Non-redundant capacity components (single uplink and servers).
Tier 2 = Tier 1 + Redundant capacity components.
Tier 3 = Tier 1 + Tier 2 + Dual-powered equipment and multiple uplinks.
Tier 4 = Tier 1 + Tier 2 + Tier 3 + all components are fully fault-tolerant including uplinks, storage, chillers, HVAC systems, servers etc. Everything is dual-powered.

APPENDIX II

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
7.1 Data Center Design and Planning	7.1.1 MCDA shall carry out site surveys to ensure a data center design is in line with the tiered reliabilities.			
	7.1.2 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, lightning, earthquake, fire etc.			
	7.1.3 MCDA shall develop a data center design with associated specifications and Bill of Quantites (BoQ)			
	7.1.4 MCDA shall ensure that relevant construction and equipment installation is done in line with the specifications and Bill of Quantites (BoQ)			
	7.1.5 MCDA shall ensure proper grounding for both lightning protection and grid power. Type 1+2 surge arrestors should be installed to protect the data center from lightning(as guided by IEC 62305-4).			
	7.1.6 Upon completion of the construction and equipment installation MCDA shall carry out the tests and the results formally documented.			
	7.1.7 MCDA shall ensure that the 'as built' physical and logical designs of the data center are documented.			
	7.1.8 MCDA shall ensure that the data center project is commissioned and a Completion Certificate issued.			
	7.1.9 Physical and logical designs shall be updated whenever changes occur.			
	7.1.10 MCDA shall ensure that the Data center is designed with flexible and adequate "white space" empty space that can accommodate future racks and cabinets. The space sorrounding the data center must also be considered for future expansion (the facility specifications should be in line with TIA-942 standard).			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	7.1.11 MCDA shall ensure that the data center includes the following key functional areas (as guided by TIA-942); an Entrance Room, Main Distribution Area (MDA), Horizontal Distribution Area (HDA), Zone Distribution Area (ZDA) and Equipment Distribution Area (EDA) as minimum functional areas. The data center should also have a staging area for unpacking and possibly for testing new equipment before deploying them in the computer room.			
8.0 Planning Layout 8.1 Whitespace	12.4.1 A data center shall be designed with plenty of flexible white space that can accommodate future racks or cabinets.			
	12.4.2 The space around the data center must be considered for future growth and planned for easy annexation.			
	12.4.3 MCDA shall ensure that there is adequate space between the racks/cabinets. The layout should have both hot and cold aisles with a minimum of 1.2 meter for the cold aisle and a minimum of 1.0 meters on the hot aisle.			
	12.4.4 Wrist strap ports shall be attached to the rack by a means that ensures electrical continuity to ground for static discharge.			
	12.4.5 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 the applicable building codes for the relevant institutions charged with building approvals.			
	12.4.6 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.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	12.4.7 Every data center shall fall under any of the tiers as per TIA-942 Standard that will be determined from Appendix 1.			
8.0 Planning Layout 8.2 Cooling	8.2.1 There shall be adequate cooling equipment as well as raised floor/ overhead cable tray for more flexible cooling.			
	8.2.2 The cabinets and racks shall be arranged in an alternating pattern to create hot and cold aisle.			
	8.2.3 The air-conditioning system shall be designed to provide the design temperature and humidity conditions recommended by the manufacturers of the servers to be installed within the data center.			
	8.2.4 A 24/7/365 dedicated HVAC system with automatic dampers and connected to a backup generator			
	8.2.5 MCDA shall ensure when building new offices/identifying occupation of a new premises that considerations are made for a provision of a floor that meets the data center required minimum height (18 inches). The recommended rack and cabinet height shall be 2.4 m (8 ft.). Racks and cabinets shall preferably be no taller than 2.1 m (7 ft.) for easier access to the equipment or connecting hardware installed at the top.			
8.3 Power	8.3.1 Power requirements shall be based on the desired reliability tier as per tiered reliability standard- (See Appendix 1) and may include two or more power feeds from the utility, UPS, Multiple circuits to systems and equipment, and on-site generators.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	8.3.2 Power requirements shall be estimated for all the existing devices and for devices anticipated in the future.			
	8.3.3 Power estimation must be made to accommodate required redundancy and future growth.			
	8.3.4 Every data center shall be supported by generator(s) and UPS System(s) and shall be designed to supply the harmonic current imposed by the UPS system or computer equipment loads. The UPS batteries should be able to support the computer systems for at least 8 hr.			
	8.3.5 Data Centre shall have a Power Distribution Units (PDUs) for distribution to critical electronic equipment.			
	8.3.6 MCDA are encouraged to consider the use of green power to cut on cost of power consumption			
	8.3.7 Data center shall at all times have fire detection, extinguisher and suppression systems.			
8.4 Fire Detection and Suppression	8.4.1 The data center construction shall be separated from other occupancies by fire resistant rated construction (not less than an hour). Every opening in the fire resistant construction shall be protected to limit spread of fire and to restrict the movement of smoke from one side to the other.			
	8.4.2 Automatic detection material shall be installed to provide early fire warning and the equipment used shall be a listed smoke detection type system. The alarms and trouble signals of automatic detection or extinguishing system shall be arranged to annunciate in a constantly occupied location.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	8.4.3 MCDA shall ensure that the IT personnel designated to man the facility are continually and thoroughly trained in the functioning of the alarm system, desired response to alarm condition, location of emergency equipment, tools and all available extinguishing equipment.			
	8.4.4 MCDA shall ensure that appropriate extractor fans are installed to extract any gas discharge / leakage.			
	8.4.5 The fire protection systems and hand-held fire extinguishers shall comply with NFPA-75			
9.0 Cabling Infrastructure **9.1 Whitespace**	9.1.1 Data centers shall use a minimum laser-optimized 50 microns multimode fiber for backbone cabling and with minimum 24 cores backbone cable.			
	9.1.2 Data centers shall use the highest capacity horizontal cabling media available as recommended by the current IEEE 802.3 standards to reduce the need for re-cabling in the future			
	9.1.3 A data center shall be designed with separate racks and pathways for each media type. The power and communication cables shall be separated on different pathways or separated by a physical barrier.			
	9.1.4 Adequate space must be provided within and between racks, the cabinet and the pathways for better cable management, bend radius protection, and access.			
	9.1.5 A labeling scheme for all racks, cabinets, patch panels, patch cords and cables must be maintained.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	9.1.6 Branch circuits in data centers shall be in watertight flexible metal conduit. Feeder circuits to power distribution units and panels shall be installed in solid metal conduit. If the feeder circuits are not in solid metal conduit, they should be in watertight flexible metal conduit.			
	9.1.7 In data centers that use overhead cable trays, the normal separation distances provided by standard practices provides adequate separation. As specified in ANSI/TIA-569-B, a minimum of 300 mm (12 in) access headroom between the top of a tray or runway and the bottom of the tray or runway above shall be provided and maintained.			
	9.1.8 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. Where this is not possible, horizontal and vertical separation of power and telecommunications cables shall be provided.			
	9.1.9 In addition, vertical separation shall be provided by placing the telecommunications cabling in cable trays or baskets as far above the power cables as possible, preferably with the top of the cable tray or basket 20 mm (0.75 in) below the bottom of the access floor tile; in the equipment cabinet aisles, allocate separate aisles for power and telecommunications cabling as maybe applicable..			
	9.1.10 Current alternate standard to raised floor			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	9.1.11 Cables shall not be left abandoned under the access floor or in overhead cable trays and shall be terminated on at least one end in the main distribution area or a horizontal distribution area, or removed.			
	9.1.12 Planning of 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. Lighting fixtures and sprinkler heads should be placed between cable trays, not directly above cable trays.			
	9.1.13 There should be full redundancy in the data center network; Use two or more ISPs and pairs of IT equipment.			
10.0 Environment and Ambience 10.1 Physical	10.1.1 The room shall be protected from contaminants in accordance with ANSI/TIA-569-B.			
	10.1.2 The Building design shall guard against excessive computer room vibration.			
	10.1.3 Floors, walls and ceiling shall be sealed, painted or constructed of a material to minimize dust.			
	10.1.4 Walls, floors and ceilings shall be light in color to enhance room lighting. Floors shall have anti-static properties as per IEC 61000-4-2.			
	10.1.5 Sprinkler systems in computer rooms shall be pre-action systems, where risk of water ingress exists, a means of evacuating water from the space shall be provided (e.g. a floor drain). Any water and drain pipes that run through the room should be located away from and not directly above equipment in the room.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	10.1.6 Equipment should be placed in cabinets and racks with "cold" air intake at the front of the cabinet or rack, and "hot" air exhaust out the back.			
	10.1.7 Blank panels should be installed in unused rack and cabinet spaces to improve the functioning of "hot" and "cold" aisles. Perforated access floor tiles should be located in the "cold" aisles rather than in the "hot" aisles to improve the functioning of the "hot" and "cold" isles.			
	10.1.8 A minimum of 1 m (3 ft.) of front clearance shall be provided for installation of equipment. A front clearance of 1.2 m (4 ft.) is preferable to accommodate deeper equipment. A minimum of 0.6 m (2 ft.) of rear clearance shall be provided for service access at the ear of racks and cabinets. A rear clearance of 1 m (3 ft.) is preferable. Some equipment may require service clearances of greater than 1 m (3 ft.) as may be guided by equipment manufacturer requirements.			
	10.1.9 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.			
	10.1.10 Access to the data Centre shall require protective gears/garments to minimize dust and other risks.			
	10.1.11 The data Centre building shall conform to all applicable national, state, and local codes.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
	10.1.12 Where the building is not dedicated to the data center, other tenant spaces should be non-industrial, International Building Code type 'B' offices, and non-intrusive to the data center. Avoid buildings with restaurants and cafeterias to minimize fire risk.			
	10.1.13 If the data center is to be on an upper floor of a multi-tenant building, then there shall be adequate shaft and conduit space for generator, security, telecommunications, and electrical conduits as well as supplemental HVAC, grounding conductors and cabling to antennas, as needed.			
	10.1.14 The building hosting the data Centre shall not be in the flight path of any nearby airports. The building shall be no closer than 0.8 km (½ mile) from a railroad or major interstate highway. The building shall not be within 0.4 km (¼ mile) of an airport, research lab, chemical plant, landfill, river, coastline, or dam as applicable. The building shall not be located adjacent to a foreign embassy the building shall not be located in high crime areas.			
10.2 Cooling	10.2.1 There shall be adequate cooling equipment as well as raised floor system for more flexible cooling as may be appropriate.			
	10.2.2 The air-conditioning system shall be designed to provide temperature and humidity conditions recommended by equipment manufacturers. The temperature and humidity shall be controlled to provide continuous operating ranges for temperature and humidity.			
	10.2.3 There shall be a 24/7 dedicated HVAC system with automatic dampers and connected to a backup generator.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
10.3 Power	10.3.1 Power requirements will be based on the desired reliability as per tiered reliability standard – Appendix 1.			
	10.3.2 The power system shall be supported by at least two standby generator system. Where batteries are used for backup, adequate ventilation and spill containment as required shall be provided.			
11.0 Physical Security	11.1 The perimeter of the site shall be protected by appropriate intruder detection system and monitored by visible or infrared Closed Circuit Television (CCTV) system. All common areas shall be monitored, including parking lots, loading docks, and building entrances.			
	11.2 Access to the site shall be secured by identification and authentication systems.			
	11.3 There shall be only one single point of entry. Consideration can be made for physical access control with anti-tailgating / anti-pass-back turn-style gate that permits only one person to pass at any one time after authentication.			
	11.4 The security of information at the data center should be in line with; information security standard, ISO 27001/2, and the computer misuse and cybercrime Act 2018			
12.0 Data Center Monitoring	12.1 MCDA shall ensure that monitoring system are installed to check the health status of all the active and computing devices.			
	12.2 MCDA shall install a monitoring tool to check on the data center environment i.e. temperature, humidity and power.			
	12.3 MCDA shall install a real time monitoring system to check the Physical security of the data center.			

SUB TOPIC	DETAILS	RATING		
		YES	NO	%
13.0 Maintenance and SLAs	13.1 All the components of the data center shall be tested periodically once the data center is in operation to ensure that they will continue to function properly. The records for the test shall be kept always.			
	13.2 Maintenance programs shall be identified to detect imminent or conditional failures for all data center equipment and service tags / maintenance schedule.			
	13.3 MCDA shall ensure Service Level Agreement (SLA) are maintained with a minimum of data center services availability of 99.99%	.		

DATA CENTRE STANDARD WORKING GROUP
ALEX NJIHIA- ICTA
DR. CHARLES BORURA- KRA
ELIAKIM MZUNGU-ICTA
ELIJAH CHERUIYOT- ICTA
ANTONY MURAGURI- ICTA

ICT Authority

Telposta Towers, 12th Floor, Kenyatta Ave

P.O. Box 27150 - 00100 Nairobi, Kenya

t: + 254-020-2211960/62

Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke

Visit: www.icta.go.ke

Become a fan: www.facebook.com/ICTAuthorityKE

Follow us on twitter: @ICTAuthorityKE