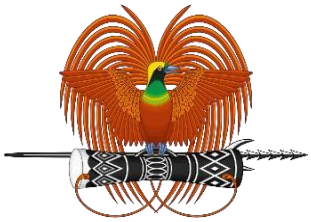


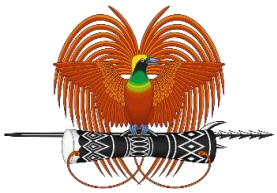
Papua New Guinea

Department of Information and Communication Technology

Government Data Centre Standards, Guidelines and Specifications 2025

Document Control:

Document Name	PNG Government Data Centre Standards, Guidelines and Specifications 2025
Custodian	Department of Information and Communication Technology
Edition	Draft 3
Approved By	
Date Approved	
Effective Date	
Next Review Date	



PNG Government Data Centre Standards, Guidelines and Specifications 2025

Table of Contents

1. Introduction to the standard 8

1.1 Scope 8

1.2 Purpose 8

1.3 Objectives 9

1.4 Explanation of its purpose and significance 11

1.5 Applicability to different types of data centers 12

2. Normative References 12

3. Definitions 14

General Requirements 20

4. 1 Compliance and Adherence to Local Regulations and Laws: 20

- Standard 4.1.1: 20
- Standard 4.1.2: 20
- Standard 4.1.3: 21

4.2 Environmental Considerations and Sustainability: 21

- Standard 4.2.1: 21
- Standard 4.2.2: 23
- Standard 4.2.3: 23
- Standard 4.2.4: 24

4.3 Safety Guidelines for Personnel Working in the Data Center: 24

- Standard 4.3.1: 24
- Standard 4.3.2: 25
- Standard 4.3.3: 25

- Standard 4.3.4: 25

4.4 Accessibility and Usability Considerations for Differently-Abled Individuals: 26

- Standard 4.4.1: 26
- Standard 4.4.2: 26
- Standard 4.4.3: 26
- Standard 4.4.4: 26

5. Infrastructure and Facility Design 26

5.1 Physical Location and Site Selection Considerations: 26

- Standard 5.1.1: 26
- Standard 5.1.2: 27
- Standard 5.1.3: 27

5.2 Building and Structural Requirements: 27

- Standard 5.2.1: 27
- Standard 5.2.2: 27
- Standard 5.2.3: 27

5.3 Power Supply and Distribution Guidelines: 27

- Standard 5.3.1: 27
- Standard 5.3.2: 28
- Standard 5.3.3: 28

5.4 Cooling and Ventilation System Specifications: 28

- Standard 5.4.1: 28
- Standard 5.4.2: 28
- Standard 5.4.3: 28

5.5 Fire Detection and Suppression System Guidelines: 28

- Standard 5.5.1: 28

- Standard 5.5.2: 28
- Standard 5.5.3: 28

5.6 Physical Security Measures and Access Control: 29

- Standard 5.6.1: 29
- Standard 5.6.2: 29
- Standard 5.6.3: 29

Data Center Hardware and Equipment 29

6.1 Server Equipment Standards: 29

- Standard 6.1.1: 29
- Standard 6.1.2: 29
- Standard 6.1.3: 29

6.2 Networking Equipment Requirements: 30

- Standard 6.2.1: 30
- Standard 6.2.2: 30
- Standard 6.2.3: 30

6.3 Storage System Guidelines: 30

- Standard 6.3.1: 30
- Standard 6.3.2 30
- Standard 6.3.3: 31

6.4 Redundancy and Backup Procedures: 31

- Standard 6.4.1: 31
- Standard 6.4.2: 31
- Standard 6.4.3: 31

6.5 Equipment Installation and Maintenance Protocols: 31

- Standard 6.5.1: 31

- Standard 6.5.2: 31
- Standard 6.5.3: 31

Information Security and Data Protection 32

7.1 Data Privacy and Confidentiality Requirements: 32

- Standard 7.1.1: 32
- Standard 7.1.2: 32
- Standard 7.1.3: 32

7.2 Cybersecurity Measures and Best Practices: 32

- Standard 7.2.1: 32
- Standard 7.2.2: 33
- Standard 7.2.3: 33

7.3 Incident Response and Reporting Procedures: 33

- Standard 7.3.1: 33
- Standard 7.3.2: 33
- Standard 7.3.3: 34

7.4 Data Backup and Disaster Recovery Planning: 34

- Standard 7.4.1: 34
- Standard 7.4.2: 34
- Standard 7.4.3: 35

Monitoring and Performance 35

8.1 Monitoring and Tracking of Data Center Performance: 35

- Standard 8.1.1: 35
- Standard 8.1.2: 35
- Standard 8.1.3: 36

8.2 Key Performance Indicators (KPIs) and Metrics to Assess Efficiency: 36

- Standard 8.2.1: 36
- Standard 8.2.2: 36
- Standard 8.2.3: 37

8.3 Capacity Planning and Scalability Considerations: 37

- Standard 8.3.1: 37
- Standard 8.3.2: 37
- Standard 8.3.3: 37

Documentation and Reporting 38

9.1 Documentation Requirements for Data Center Operations: 38

- Standard 9.1.1: 38
- Standard 9.1.2: 38
- Standard 9.1.3: 38

9.2 Reporting Obligations to Regulatory Authorities: 38

- Standard 9.2.1: 38
- Standard 9.2.2: 38
- Standard 9.2.3: 38

9.3 Change Management and Audit Procedures: 38

- Standard 9.3.1: 38
- Standard 9.3.2: 39
- Standard 9.3.3: 39

Compliance and Certification 39

10.1 Requirements for Data Centers to Achieve and Maintain Certification: 39

- Standard 10.1.1: 39
- Standard 10.1.2: 39
- Standard 10.1.3: 39

10.2 Procedures for Evaluating Compliance with the Standard: 40

- Standard 10.2.1: 40
- Standard 10.2.2: 40
- Standard 10.2.3: 40

10.3 Oversight and Auditing Processes: 40

- Standard 10.3.1: 40
- Standard 10.3.2: 41
- Standard 10.3.3: 41

Annexes 42

1. Introduction to the standard

Introduction to the Standard: The data center standard for Papua New Guinea's government departments is a set of established guidelines and rules that detail how data centers owned by government entities should be designed, built, and operated. These standards aim to ensure that the government's data centers are efficient, secure, and reliable.

1.1 Scope

The scope of the data center standards for Papua New Guinea's government departments encompasses the design, construction, operation, and maintenance of data centers utilized by various government agencies. It includes the physical infrastructure, such as power, cooling, and security systems, as well as the virtual components, including servers, networks, and data storage. The scope also extends to procedures for disaster recovery, data backup, and compliance with relevant regulations.

1.2 Purpose

The purpose of establishing these data center standards for Papua New Guinea's government departments is to achieve several significant goals:

- **Efficiency:** By outlining best practices for data center design and operation, the standards aim to increase the efficiency of government data centers. This includes optimizing energy usage, reducing waste, and improving overall resource utilization.

- **Security:** Ensuring data security is paramount. These standards set guidelines to safeguard sensitive government information from cyber threats, unauthorized access, and data breaches. This includes the physical and logical security measures, such as locks, cameras, firewalls, encryption, and authentication that protect the data center from unauthorized access, theft, damage, or cyberattacks.

- **Reliability:** The standards contribute to the reliability of government services by specifying redundancy and fail-safe mechanisms, minimizing downtime, and maximizing uptime of critical systems.
- **Interoperability:** Following consistent standards across different government departments helps enhance interoperability, making it easier for various agencies to share data and collaborate effectively.
- **Cost Savings:** Adhering to standardized practices can lead to cost savings through efficient resource allocation, reduced energy consumption, and streamlined maintenance procedures.
- **Scalability:** The standards provide a framework that supports the scalability of data center infrastructure, allowing for growth and adaptation to changing technological demands.
- **Compliance:** Government departments must adhere to regulatory and compliance requirements. These standards ensure that data centers meet these obligations, avoiding legal issues and potential penalties.
- **Service Quality:** By adhering to the standards, government agencies can provide citizens with reliable and high-quality digital services, leading to increased satisfaction and trust.

1.3 Objectives

1. **Ensure Data Security:** Establish security protocols and best practices to safeguard sensitive data, protect against cyber threats, and maintain the confidentiality, integrity, and availability of data stored and processed in data centers.
2. **Promote Reliability and Availability:** Set standards for infrastructure design, redundancy, and disaster recovery planning to ensure data centers maintain high levels of availability and can withstand disruptions without compromising operations.
3. **Enhance Energy Efficiency:** Define energy efficiency guidelines to minimize environmental impact and optimize energy consumption, promoting sustainability in data center operations through technologies and practices like virtualization, efficient cooling systems, and power management.
4. **Facilitate Scalability:** Provide guidelines for scalability planning, allowing data centers to adapt to increasing demands and technological advancements without compromising performance or efficiency.
5. **Ensure Compliance:** Establish compliance requirements that align with local and international regulations, ensuring data centers adhere to legal and industry standards to prevent legal and reputational risks.
6. **Encourage Innovation:** Foster innovation and digital transformation for businesses and organization by promoting the adoption of cutting-edge technologies, best practices, and emerging trends to keep data centers at the forefront of technological advancements.
7. **Standardize Processes:** Define standardized procedures and processes for data center management, operations, maintenance, and incident response to enhance consistency and effectiveness.
8. **Support Economic Growth:** Contribute to the growth of the digital economy by providing a robust framework that encourages investment in data center infrastructure, attracting local and foreign businesses looking for secure and reliable data hosting solutions.

9. **Provide Consumer Confidence:** Enhance consumer trust by ensuring data centers meet high standards of security, reliability, and operational excellence, ultimately benefiting individuals, businesses, and government entities relying on data center services.
10. **Facilitate Cross-Border Data Transactions:** Establish guidelines that align with international data protection and security standards, enabling seamless cross-border data transfers while ensuring data sovereignty and privacy are upheld.
11. **Encourage Collaboration:** Foster collaboration among data center operators, industry stakeholders, and regulatory bodies to share knowledge, best practices, and expertise to continuously improve the data center landscape in PNG.

1.4 Explanation of its purpose and significance

Explanation of Purpose and Significance: The purpose of these standards is to create a consistent and reliable framework for designing and managing government data centers. They are crucial because they help ensure that the digital infrastructure is well-organized, secure from cyber threats, and operates smoothly. Adhering to these standards can lead to cost savings, better data management, and improved services for citizens as government departments increasingly rely on digital systems for various functions.

Significance of a Data Center is to “support business operations” and provide services such as data storage, management, backup and recovery, productivity applications, e-commerce transactions, online gaming, big data, machine learning and artificial intelligence.

Data Center can also offer services such as cloud computing, colocation, disaster recovery, and virtualization to its customers. A datacenter requires a lot of resources

and infrastructure to function properly, such as power supply, cooling system, racks and cabinets, cabling, and monitoring and management tools.

1.5 Applicability to different types of data centers

Applicability to Different Types of Data Centers: These standards are designed to be adaptable to various types of data centers within government departments. Whether it's a large central data center serving multiple departments or smaller data centers specific to individual agencies, the guidelines can be tailored to suit the unique needs and capacities of each type of data center. This flexibility allows for consistent improvements in efficiency and security across the government's digital infrastructure landscape.

2. Normative References

*2.1 List of relevant international and national standards and guidelines that apply to data centers in Papua New Guinea. **

- **ISO/IEC 27001**: Information Security Management System (ISMS) - Requirements for establishing, implementing, maintaining, and continually improving an ISMS within the context of the organization.
- **ISO/IEC 27002**: Code of Practice for Information Security Controls - Provides guidelines for implementing information security controls based on best practices and security risk management.
- **ISO/IEC 20000**: IT Service Management - Specifies requirements for the service provider to deliver managed services effectively, meeting agreed service requirements.

- ISO/IEC 22301: Societal Security - Business Continuity Management Systems - Requirements - Provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving a business continuity management system.
- ISO 9001: Quality Management System - Requirements - Sets out the criteria for a quality management system and is based on a number of quality management principles including a strong customer focus, the involvement of top management, and a process approach.
- ISO/IEC 11801: Information Technology - Generic Cabling for Customer Premises - Specifies the requirements for balanced cabling systems for use in premises that support various services.
- ISO/IEC 30134: Information Technology - Governance of IT - Evaluation of the Governance of Information Technology - Provides guidelines for evaluating the governance of IT within organizations. This standard can also be applied to operations and maintenance of Data Centers. Which specifies key performance indicators for Data Center resource efficiency, such as Power Usage Efficiency (PUE), Renewable Energy Factor (REF), IT Equipment Energy Efficiency (ITEE)
- TIA-942: Telecommunications Infrastructure Standard for Data Centers - Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms.
- ASHRAE Standard 90.4: Energy Standard for Data Centers - Provides minimum energy efficiency requirements for the design and operation of data centers.
- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations - Provides a catalog of security and privacy controls for federal information systems and organizations.
- EN 50600 series: An International series of Data Center Standards in continuous development. It covers various aspects of Data Center facilities and infrastructures, such as power supply, cooling, cabling, security, management

and key performance indicators. This standard also defines four “Availability Classes”, from 1-4, that rate the facilities according to their expected downtime per year.

- **Uptime Institute Tier Classification System**: It is a performance-based approach for determining the facility’s resiliency in terms of four levels of redundancy/reliability. It evaluates the Data Center during the design, construction and commissioning phases, and certifies the facility according to its standards.
- **ISO 50001**: Energy Management System (EMS) - It specifies requirements for establishing, implementing, maintaining and improving an energy management system (EMS). The intended outcome is to enable an organization to follow a systematic approach in achieving continual improvement of energy performance and the EMS.

3. Definitions

Terms within the standards that need defining.

Terms	Definitions
1. Access Control	Regulating resource access based on authorization levels.
2. Accessibility	Enabling use by diverse abilities, including disabilities.
3. Availability	Continuous resource functionality and accessibility.

4. Backup and Archival Strategy	Planned data redundancy and storage approach.
5. Backup Strategy Templates	Predefined plans for data backup scheduling.
6. Capacity Assessment Methodology	Systematic resource utilization evaluation.
7. Collaboration	Effective teamwork and cross-functional cooperation.
8. Compatibility Assessment	Evaluation of new components' integration with existing systems.
9. Compliance	Adherence to industry regulations and standards.
10. Confidentiality	Safeguarding sensitive data from unauthorized access.
11. Cyber threats	Malicious activities targeting data security.
12. Data backup	Creating duplicate data copies for recovery purposes.
13. Data center	Facility housing computing equipment and systems.
14. Data Classification	Categorizing data by sensitivity and importance.
15. Data Privacy	Protecting personal information in line with regulations.

16. Data sovereignty	The concept that data is subject to the laws and regulations of the country where it is collected or stored, ensuring compliance with local data protection and privacy laws.
17. Disaster recovery	The comprehensive plan and procedures for recovering business functions and data after a disruptive event, such as a natural disaster or cyberattack.
18. Disaster Recovery Plan Template	A prepared document outlining steps to recover systems and data after a disaster, guiding actions to resume normal operations.
19. Early Detection Systems	Technologies to identify and alert about potential security threats in their early stages for timely mitigation.
20. Efficiency	Optimizing resource use to achieve desired outcomes while minimizing waste.
21. Efficiency Metrics	Measurable indicators assessing resource use and operational effectiveness.
22. Energy Optimization	Energy Optimization: Improving energy efficiency and reducing consumption in data center operations.

23. **Fire Suppression Mechanisms**	Systems for quickly detecting and extinguishing fires in data centers.
24. **Forensic Analysis Procedures Checklist**	A step-by-step checklist for systematic post-incident forensic analysis.
25. **Government agencies**	Organizations overseeing regulatory aspects, including data protection and cybersecurity.
26. **Infrastructure**	Physical and virtual components supporting data center operations.
27. **Interoperability**	Systems' ability to work together, ensuring compatibility and efficient communication.
28. **Intrusion Detection and Prevention**	Systems monitoring network traffic to identify and prevent unauthorized access.
29. **Key Performance Indicators (KPIs) Reference Sheet**	Document explaining KPIs for data center efficiency evaluation.
30. **Load Balancing**	Distributing workloads across resources to ensure optimal utilization and performance.
31. **Metrics Monitoring**	Tracking and analyzing key efficiency indicators for continuous improvement.
32. **Multi-Layered Security**	Multiple security measures to safeguard data centers.

33. Network Infrastructure Planning	Strategically deploying network equipment for optimal performance and reliability.
34. Personal Protective Equipment (PPE)	Gear for personnel safety, including helmets and suits.
35. Power management	Efficiently controlling energy use in data centers.
36. Redundancy	Building systems with backup components to prevent failure.
37. Regulatory Compliance Reference Sheet	Document summarizing regulations relevant to data centers.
38. Renewable Energy	Sustainable power sources like solar or wind.
39. Resource utilization	Efficiently using computing and energy resources.
40. Safety Protocols	Comprehensive procedures ensuring personnel safety.
41. Scalability	The ability of a system or infrastructure to handle increasing workloads or demands by adding resources or components without compromising performance.

42. Scalability Considerations	Factors that need to be taken into account when planning for the ability of a system to scale, including performance, resource allocation, and architecture design.
43. Security Implementation	The process of integrating security measures, protocols, and technologies to protect data and systems from unauthorized access, breaches, and cyber threats.
44. Server Procurement	he process of acquiring, purchasing, or provisioning server hardware to meet the computing needs of a data center or organization
45. Specialized Training	Training programs designed to provide specialized knowledge and skills to personnel, enabling them to handle specific tasks or situations effectively.
46. Storage System Guidelines	Guidelines outlining best practices for designing, deploying, and managing storage systems to ensure data integrity, availability, and performance
47. Third-Party Data Sharing	Sharing data with external entities or organizations while ensuring compliance with data protection regulations and contractual obligations

48. User Interface Prioritization	Giving importance to designing digital interfaces, control panels, and applications that are accessible, user-friendly, and meet the needs of diverse users.
49. Virtualization	The process of creating virtual instances of computing resources, such as servers, storage, or networks, to improve resource utilization and flexibility.
50. Vulnerability Assessments	Systematic evaluations conducted to identify security vulnerabilities, weaknesses, or flaws in software, systems, or networks that could be exploited by attackers.

General Requirements

4. 1 Compliance and Adherence to Local Regulations and Laws:

- Standard 4.1.1: Regulatory Alignment
- All data center practices and operations shall be meticulously aligned with the latest local regulations and laws.
- Standard 4.1.2: Routine Maintenance and Audits
- Regular audits shall be conducted to confirm ongoing compliance and promptly address any deviations. Audits should be conducted on a quarterly basis, or as otherwise deemed appropriate based on the specific data center's size, complexity, and operational requirements. The frequency of audits ensures that potential deviations from established standards and practices are identified and addressed in a timely manner.

- Standard 4.1.3: Collaborative Compliance
- Collaboration with legal experts shall be maintained to interpret and apply complex regulatory changes effectively.

4.2 Environmental Considerations and Sustainability:

- Standard 4.2.1: Proactive Energy Optimization
- A proactive strategy as listed below ought to be followed to optimize energy consumption within the data center environment:

1. **Equipment Efficiency Assessment:**

♦ Regularly assess the energy efficiency of all data center equipment, including servers, cooling systems, and power distribution units.

♦ Replace older, less efficient equipment with newer, more energy-efficient models.

♦ Utilize energy-efficient hardware and technologies, such as Energy Star-rated devices.

2. **Virtualization and Consolidation:**

♦ Implement server virtualization to consolidate workloads and reduce the number of physical servers.

♦ Use virtual machines to efficiently allocate resources and prevent underutilization of hardware.

3. **Dynamic Power Management:**

♦ Implement power management policies that dynamically adjust power levels based on workload demand.

♦ Utilize tools that allow for real-time monitoring and adjustment of power consumption.

4. **Cooling Efficiency:**

- Optimize cooling system design to ensure proper airflow and temperature regulation.
- Implement hot and cold aisle containment to prevent mixing of hot and cold air streams.
- Use efficient cooling methods, such as free cooling and liquid cooling technologies.

5. Energy-efficient Lighting and Infrastructure:

- Use LED lighting and motion sensors in non-occupied areas to reduce lighting energy consumption.
- Implement energy-efficient building infrastructure, including insulation, roofing, and windows.

6. Renewable Energy Integration:

- Explore the feasibility of integrating renewable energy sources such as solar, wind, or hydroelectric power.
- Supplement data center energy consumption with clean energy alternatives.

7. Power Monitoring and Analytics:

- Implement power monitoring and analytics tools to track energy usage and identify inefficiencies.
- Analyze data to make informed decisions about energy optimization strategies.

8. Employee Awareness and Training:

- Train data center staff on energy-efficient practices and the importance of minimizing energy consumption.
- Foster a culture of energy consciousness and responsibility among personnel.

9. Regular Review and Improvement:

- Conduct periodic assessments of the energy optimization strategy's effectiveness.
- Continuously monitor advancements in energy-efficient technologies and practices for potential integration.

- Standard 4.2.2: Energy-Efficient Technologies
- Regular evaluation and adoption of energy-efficient technologies like the ones listed below shall be pursued to reduce the ecological footprint.

1. Hardware Virtualization:

- Hardware virtualization involves running multiple virtual servers on a single physical server, allowing for better utilization of hardware resources.
- This technology reduces the number of physical servers required, leading to lower energy consumption, less heat generation, and reduced space requirements.

2. Economizer Cooling Systems:

- Economizer cooling systems utilize outside air, when the environmental conditions are favorable, to cool the data center instead of relying solely on energy-intensive mechanical cooling.
- This approach reduces the reliance on traditional air conditioning systems, leading to significant energy savings.

3. Solid-State Drives (SSDs):

- SSDs consume less power compared to traditional hard disk drives (HDDs) as they have no moving parts and require less energy to operate.
- Implementing SSDs in storage systems can lead to reduced energy consumption and faster data access times.

- Standard 4.2.3: Metrics Monitoring
- Data center efficiency metrics shall be monitored closely, with periodic reporting mechanisms as follows.

♦ **Selection of Key Metrics:**	♦ Choose important efficiency metrics such as PUE, ERE, and IT Equipment Utilization that align with energy optimization goals.
♦ **Monitoring Tools and Systems:**	♦ Implement tools like energy management software and sensors to collect real-time data on chosen metrics.
♦ **Regular Data Collection:**	♦ Collect data consistently on a predetermined schedule, ensuring accuracy and reliability.
♦ **Data Analysis and Interpretation:**	♦ Analyze gathered data to spot trends, anomalies, and areas needing improvement.
♦ **Periodic Reporting:**	♦ Develop a reporting system to share analyzed metric data at defined intervals with stakeholders, showing progress and areas for enhancement.

- Standard 4.2.4: Renewable Energy Exploration
- Exploration of partnerships with renewable energy providers shall be conducted to augment sustainability efforts.

4.3 Safety Guidelines for Personnel Working in the Data Center:

- Standard 4.3.1: Comprehensive Safety Protocols

- Comprehensive safety protocols shall be developed and enforced to safeguard the well-being of data center personnel.

Key Elements of Comprehensive Data Center Safety Protocols

1. Identify and assess risks.
2. Develop clear safety protocols.
3. Provide thorough personnel training.
4. Establish emergency response plans.
5. Ensure proper personal protective equipment (PPE) usage.
6. Conduct regular safety drills and audits.

- Standard 4.3.2: Specialized Training
- Specialized training shall be provided to all staff to ensure their competency in handling emergencies and adhering to safety measures. This training includes proper response to fire incidents, including the use of fire extinguishers and evacuation procedures.
- Standard 4.3.3: Personal Protective Equipment (PPE)
- This includes providing personnel with appropriate PPE, ensuring its availability, conducting regular inspections, and enforcing its correct usage to mitigate potential risks.
- Standard 4.3.4: Safety Drills
- These drills involve simulated emergency scenarios such as fires, power outages, and evacuations. The drills should be conducted at planned intervals to test the effectiveness of emergency procedures, familiarize personnel with response protocols, and identify areas for improvement in the safety plan

4.4 Accessibility and Usability Considerations for Differently-Abled Individuals:

- Standard 4.4.1: Accessibility Integration
- This involves incorporating features that enable access for individuals with disabilities, including wheelchair ramps, accessible restrooms, tactile signage, and other accommodations, making the data center accessible and usable by all.
- Standard 4.4.2: Collaborative Design
- This collaboration ensures that the data center's physical layout, infrastructure, and amenities are designed in line with universal design principles, accommodating people of all abilities and providing equal access.
- Standard 4.4.3: User Interface Prioritization
- The development of user interfaces that cater to varying abilities and preferences shall be prioritized. This means creating digital interfaces, control panels, and applications that are designed with accessibility features such as screen reader compatibility, adjustable font sizes, and simplified navigation, ensuring that users with different abilities can interact effectively.
- Standard 4.4.4: Audits and Feedback
- Regularly evaluating the data center's accessibility features, receiving input from individuals with diverse abilities, and addressing their needs through ongoing improvements contribute to creating an environment that is welcoming and accommodating for everyone.

5. Infrastructure and Facility Design

5.1 Physical Location and Site Selection Considerations:

- Standard 5.1.1: Careful Evaluation of Geographic Factors

- The selection of data center locations must involve a comprehensive assessment of geographic factors, including seismic activity, flood risk, and proximity to natural disaster-prone areas.
- Standard 5.1.2: Accessibility and Connectivity
- Data center sites should prioritize proximity to major transportation hubs and telecommunication networks to ensure reliable connectivity.

.

- Standard 5.1.3: Zoning and Land Use Regulations
- Compliance with local zoning regulations and land use policies is imperative to secure necessary permits and approvals.

5.2 Building and Structural Requirements:

- Standard 5.2.1: Construction Material and Design
- The construction materials used in data center buildings must ensure structural integrity and durability under various conditions.
- Standard 5.2.2: Seismic Design and Mitigation
- Data center structures must be designed and engineered to withstand seismic events, with appropriate seismic hazard assessment.
- Standard 5.2.3: Load-Bearing Capacity
- Building designs should accommodate the weight of equipment, cooling systems, and potential future expansions.

5.3 Power Supply and Distribution Guidelines:

- Standard 5.3.1: Redundancy and Reliability
- Data centers should have redundant power sources and distribution paths to ensure continuous operation even during power outages.

- Standard 5.3.2: Load Balancing and Capacity Planning
- Power distribution systems should be designed to handle current and projected loads while allowing for scalability.
- Standard 5.3.3: Energy Efficiency
- Power distribution systems should incorporate energy-efficient technologies to minimize wastage and optimize utilization.

5.4 Cooling and Ventilation System Specifications:

- Standard 5.4.1: Cooling Efficiency
- Cooling systems must be designed for maximum efficiency, utilizing technologies like hot and cold aisle containment. This includes chillers, air conditioners, fans, ducts, and sensors that regulate the temperature and humidity of the datacenter.
- Standard 5.4.2: Environmental Impact
- Cooling solutions should prioritize the use of eco-friendly refrigerants and consider the overall energy consumption.
- Standard 5.4.3: Scalability and Redundancy
- Cooling systems must allow for scalability to meet increasing demands while maintaining redundancy to prevent overheating.

5.5 Fire Detection and Suppression System Guidelines:

- Standard 5.5.1: Early Detection Systems
- Data centers must be equipped with state-of-the-art fire detection systems, including smoke detectors and thermal sensors.
- Standard 5.5.2: Fire Suppression Mechanisms
- Automatic fire suppression systems using clean agents or inert gases should be installed to swiftly control and extinguish fires.
- Standard 5.5.3: Regular Testing and Maintenance

- Regular testing and maintenance of fire detection and suppression systems are crucial to ensure their optimal functionality.

5.6 Physical Security Measures and Access Control:

- Standard 5.6.1: Multi-Layered Security
- Implement multi-layered physical security measures, including perimeter fencing, surveillance cameras, and security personnel.
- Standard 5.6.2: Access Control Policies
- Access to data centers should be restricted based on roles and responsibilities, with strict authorization processes.
- Standard 5.6.3: Visitor Management
- Data centers should maintain visitor logs and adhere to a thorough identification and verification process.

Data Center Hardware and Equipment

6.1 Server Equipment Standards:

- Standard 6.1.1: Server Procurement and Validation
- Procurement of server equipment shall adhere to predefined technical specifications and validation processes.
- Standard 6.1.2: Compatibility Assessment
- All server equipment shall undergo compatibility assessments with existing infrastructure components.
- Standard 6.1.3: Performance Benchmarking
- Server performance shall be regularly benchmarked against industry standards to ensure optimal functionality.

6.2 Networking Equipment Requirements:

- Standard 6.2.1: Network Infrastructure Planning
- Networking equipment shall be deployed based on a comprehensive infrastructure planning process. This includes core switches, routers, load balancers, access switches, firewall, network cables, and physical network topology, ensuring optimal performance, redundancy, and connectivity.

- Standard 6.2.2: Scalability Considerations
- Networking equipment should accommodate future scalability requirements to support data center growth. This includes ensuring modular designs, sufficient port capacity, expandable routing capabilities, and support for emerging technologies like software-defined networking (SDN) to seamlessly adapt to evolving demands.

- Standard 6.2.3: Security Implementation
- Networking equipment must be configured to implement robust security measures, including firewalls and intrusion detection. Key security implementations involve next-generation firewalls, intrusion prevention systems (IPS), VPNs for secure remote access, network segmentation, access control lists (ACLs), and threat intelligence integration to safeguard data center networks against cyber threats.

6.3 Storage System Guidelines:

- Standard 6.3.1: Storage Capacity Assessment
- Storage system specifications shall be determined based on current and projected data storage needs.
- Standard 6.3.2**:** Data Classification and Segmentation

- Storage systems shall facilitate data classification and segmentation for effective data management.
- Standard 6.3.3: Backup and Archival Strategy
- Storage systems must integrate a well-defined backup and archival strategy to ensure data redundancy.

6.4 Redundancy and Backup Procedures:

- Standard 6.4.1: Redundancy Design
- Data center hardware shall be redundantly designed to prevent single points of failure.
- Standard 6.4.2: Backup Frequency and Retention
- Backup procedures shall be established, specifying the frequency of backups and retention periods.
- Standard 6.4.3: Restoration Testing
- Regular restoration testing shall be conducted to ensure the effectiveness of backup and recovery procedures.

6.5 Equipment Installation and Maintenance Protocols:

- Standard 6.5.1: Installation Procedures
- Equipment installation shall follow approved protocols, adhering to manufacturer guidelines and best practices.
- Standard 6.5.2: Routine Maintenance Schedule
- A routine maintenance schedule shall be established to prevent hardware degradation and ensure optimal performance.
- Standard 6.5.3: Documentation and Tracking
- Thorough documentation of equipment installation, configuration changes, and maintenance activities shall be maintained.

Information Security and Data Protection

7.1 Data Privacy and Confidentiality Requirements:

- Standard 7.1.1: Data Classification and Handling
- Data shall be classified based on sensitivity, and handling procedures shall align with classification levels.
- Standard 7.1.2: Consent and Privacy Notices
- Processes for obtaining user consent and providing transparent privacy notices shall be established. Types of processes may include implementing user-friendly consent mechanisms, such as opt-in/opt-out options, ensuring clear and concise privacy policies, disclosing data collection practices, and enabling users to control their data preferences.
- Standard 7.1.3: Third-Party Data Sharing
- Sharing of data with third parties shall follow strict compliance and contractual obligations. Strict compliance includes adhering to relevant data protection regulations, ensuring data is shared only for specified purposes, obtaining explicit user consent when required, conducting due diligence on third-party data recipients, and establishing comprehensive data sharing agreements that outline responsibilities, data usage restrictions, and security measures.

7.2 Cybersecurity Measures and Best Practices:

- Standard 7.2.1: Access Control
- Implement strong access control mechanisms.
- Utilize multi-factor authentication (MFA).
- Enforce role-based access control (RBAC).
- Maintain strict password policies.
- Conduct regular access reviews.

- Standard 7.2.2: Intrusion Detection and Prevention
- Implement strong access control mechanisms.
- Utilize multi-factor authentication (MFA).
- Enforce role-based access control (RBAC).
- Maintain strict password policies.
- Conduct regular access reviews.

- Standard 7.2.3: Regular Vulnerability Assessments
- Conduct routine vulnerability assessments.
- Perform regular scans and penetration tests.
- Identify vulnerabilities in software, systems, and network.
- Promptly patch and update systems based on findings.

7.3 Incident Response and Reporting Procedures:

- Standard 7.3.1: Incident Identification and Categorization
- Develop and document clear protocols for identifying and categorizing security incidents.
- Define criteria to facilitate consistent categorization based on the severity and potential impact of incidents.
- Provide guidelines for accurately determining incident types to aid in appropriate response planning.

- Standard 7.3.2: Escalation and Notification
- Establish precise and streamlined incident escalation procedures to ensure swift and effective response.

- Define a well-defined chain of command for escalating incidents to the appropriate personnel.
- Specify notification mechanisms and timelines for informing relevant stakeholders, enabling timely collaboration and decision-making.

- Standard 7.3.3: Forensic Analysis
- Outline comprehensive procedures for conducting forensic analysis following security incidents.
- Specify methodologies for preserving digital evidence and maintaining data integrity during analysis.
- Provide guidelines for skilled forensic examination to uncover incident causes, extent, and potential system impact.
- Define steps for data recovery and system restoration post-incident, maintaining operational continuity while addressing security concerns.

7.4 Data Backup and Disaster Recovery Planning:

- Standard 7.4.1: Backup Strategy and Frequency
- Develop a comprehensive data backup strategy specifying backup frequency and retention periods.
- Define the intervals at which data backups are performed to align with data sensitivity and operational requirements.
- Set retention periods that balance data availability and storage capacity considerations.

- Standard 7.4.2: Disaster Recovery Plan
- Document a comprehensive disaster recovery plan outlining actionable steps for expedited system restoration in case of critical failures or catastrophic events.

- Detail roles, responsibilities, and communication channels for responding to disasters effectively.
- Identify critical systems, prioritize recovery processes, and establish guidelines for alternative operational modes.

- Standard 7.4.3: Periodic Testing
- Conduct regular testing of data backup and disaster recovery procedures to validate their readiness and effectiveness.
- Specify testing schedules, methodologies, and scenarios that simulate potential disaster scenarios.
- Ensure lessons learned from testing are incorporated into plan refinements and continuous improvement efforts.

Monitoring and Performance

8.1 Monitoring and Tracking of Data Center Performance:

- Standard 8.1.1: Performance Metrics Selection
- Carefully choose relevant performance metrics that provide meaningful insights into different facets of data center operations.
- Ensure metrics align with business objectives, such as power usage, cooling efficiency, server utilization, and network latency.

- Standard 8.1.2: Continuous Monitoring
- Deploy continuous monitoring processes to proactively track and analyze performance metrics in real time.
- Monitor critical parameters including temperature, humidity, power consumption, and network traffic to identify potential issues promptly.

- Monitor hardware and software tools that monitor the performance, availability, security, and efficiency of the Data Center.

- Standard 8.1.3: Real-Time Reporting
- Establish real-time reporting mechanisms to enable immediate awareness of performance anomalies.
- Implement alerting systems that notify relevant personnel when predefined thresholds are exceeded, enabling swift corrective actions to mitigate potential disruptions.
- Provide alerts, reports, analytics, and automation features to help the Data Center operator manage the Data Center efficiently.

8.2 Key Performance Indicators (KPIs) and Metrics to Assess Efficiency:

- Standard 8.2.1: KPI Definition
- Define specific key performance indicators (KPIs) that allow for quantitative evaluation of data center efficiency and overall effectiveness.
- KPIs should be directly linked to strategic objectives, such as power utilization effectiveness (PUE), resource utilization, and system availability.

- Standard 8.2.2: Metric Selection
- Carefully select relevant metrics to measure critical operational areas, including energy consumption, server utilization rates, network response times, and cooling efficiency.
- Metrics should provide actionable insights into resource usage, infrastructure performance, and service levels.

- Standard 8.2.3: Periodic Review
- Conduct regular reviews of defined KPIs and metrics to ensure their ongoing relevance and alignment with evolving data center goals and industry best practices.
- Make adjustments as needed to capture changing priorities and technological advancements accurately.

8.3 Capacity Planning and Scalability Considerations:

- Standard 8.3.1: Capacity Assessment
- Conduct regular capacity assessments to evaluate the utilization of computing resources and identify potential performance bottlenecks.
- Utilize methods such as performance monitoring, trend analysis, and utilization reports to ensure optimal resource allocation.

- Standard 8.3.2: Scalability Strategy
- Develop a well-defined scalability strategy that outlines how the data center will accommodate future growth and evolving technological demands.
- Implement horizontal scaling methods, like load balancing and clustering, to distribute workloads efficiently across multiple servers as demand increases.

- Standard 8.3.3: Resource Allocation
- Implement efficient resource allocation methodologies, including dynamic resource allocation and virtualization technologies.
- Use techniques like auto-scaling to automatically adjust resources based on workload fluctuations, ensuring optimal utilization while preventing overprovisioning or underutilization.

Documentation and Reporting

9.1 Documentation Requirements for Data Center Operations:

- Standard 9.1.1: Comprehensive Documentation
- Maintain comprehensive documentation outlining all aspects of data center operations, including infrastructure, equipment, and processes.
- Standard 9.1.2: Configuration Records
- Document configurations of hardware, software, and networking components for accurate reference and troubleshooting.
- Standard 9.1.3: Operational Procedures
- Develop and maintain documented operational procedures for routine tasks, maintenance, and emergency responses.

9.2 Reporting Obligations to Regulatory Authorities:

- Standard 9.2.1: Regulatory Reporting Framework
- Establish a framework for reporting data center activities and compliance with relevant regulations to regulatory authorities.
- Standard 9.2.2: Timely Reporting
- Ensure timely submission of required reports to regulatory bodies, addressing data security, environmental impact, and other relevant areas.
- Standard 9.2.3: Accuracy and Transparency
- Ensure accuracy and transparency in reporting by providing complete and truthful information to regulatory authorities.

9.3 Change Management and Audit Procedures:

- Standard 9.3.1: Record Retention Policy

- Maintain a formal record retention policy to store essential data center documents and records for specified periods.
- Standard 9.3.2: Audit Preparedness
- Prepare for audits by maintaining organized records, documentation, and evidence of compliance with standards and regulations.
- Standard 9.3.3: Compliance Tracking
- Regularly review and update records to ensure alignment with changing regulations and standards.

Compliance and Certification

10.1 Requirements for Data Centers to Achieve and Maintain Certification:

- Standard 10.1.1: Certification Framework
- Establish a comprehensive framework detailing the specific requirements data centers need to meet to attain and sustain certification.
- Define the scope of certification, eligibility criteria, and the assessment process involved.

- Standard 10.1.2: Documented Compliance Criteria
- Document explicit compliance criteria, processes, and industry standards that data centers must adhere to to qualify for certification.
- Outline the specific technical, operational, and security benchmarks that must be met to demonstrate compliance.

- Standard 10.1.3: Continuous Improvement Strategy

- Develop a well-structured continuous improvement strategy as an integral part of the certification process.
- Detail mechanisms for ongoing assessment, evaluation, and enhancement of data center practices to ensure sustained compliance with certification requirements

10.2 Procedures for Evaluating Compliance with the Standard:

- Standard 10.2.1: Compliance Assessment Procedures
- Develop procedures for assessing data center compliance with the established standards, covering all operational aspects.
- Standard 10.2.2: Documentation Review
- Conduct thorough reviews of documentation, records, and operational procedures to evaluate alignment with the standard.
- Standard 10.2.3: Performance Audits
- Execute periodic performance audits to assess data center practices, controls, and adherence to standards.

10.3 Oversight and Auditing Processes:

- Standard 10.3.1: Oversight Structure
- Establish a clear oversight structure responsible for ensuring data center compliance with standards and regulations. The oversight structure comprises:
- **Oversight Committee:** A multi-disciplinary team comprising representatives from different departments, including IT, facilities, security, and legal.
- **Designated Compliance Officer:** A dedicated individual responsible for coordinating compliance efforts, liaising with the committee, and reporting to higher management.
- **Regular Reporting:** Define reporting frequencies and channels to keep stakeholders informed about compliance status and potential issues.

- Standard 10.3.2: Independent Auditing
- Engage independent auditors to conduct regular assessments of data center operations, controls, and practices. Auditors perform:
- **Risk Assessments:** Identify potential compliance risks and vulnerabilities.
- **Process Audits:** Evaluate adherence to established standards and regulatory requirements.
- **Controls Review:** Assess effectiveness of internal controls, security measures, and data protection mechanisms.
- **Report Generation:** Provide comprehensive audit reports outlining findings and recommendations.

- Standard 10.3.3: Corrective Actions
- Develop procedures for addressing non-compliance findings through corrective actions and continuous improvement plans. These procedures involve:
- **Issue Identification:** Promptly identify and document non-compliance findings from audits and assessments.
- **Root Cause Analysis:** Investigate the underlying causes of non-compliance to prevent recurrence.
- **Corrective Plans:** Develop action plans outlining specific steps to rectify issues and achieve compliance.
- **Timelines:** Set clear timelines for corrective actions, prioritizing critical issues.
- **Follow-Up:** Monitor and verify the implementation and effectiveness of corrective actions.
- **Continuous Improvement:** Incorporate lessons learned into ongoing improvement strategies to prevent similar issues in the future.

Annexes

- *11.1 Additional information, examples, and guidelines to support the main content of the standard.....*