LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
CO-OPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

REVIEWED ICT DATA CENTRE PHYSICAL ACCESS AND ENVIROMENTAL CONTROL POLICY

Version: 2

Table of Contents

I. Acronyms and Abbreviations

AC	Alternating Current
CCTV	Closed Circuit Television
CoGHSTA	Cooperative Governance, Human Settlement and Traditional Affairs
GITO	Government Information Technology Office(r)
UPS	Uninterruptable Power Supply

II. Clarification of Terms

Access Control: mechanisms and policies that restrict access to resources.

Alternating Current: an electrical current that frequently reverses direction.

Biometrics: process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity.

Closed Circuit Television: the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

Data Centre: facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

Fire Extinguishers: an active fire protection device used to extinguish or control small fires, often in emergency situations.

Raised floor: a floor that provides an elevated structure above a solid substrate (often a concrete slab) to create a hidden void for the passage of mechanical and electrical services.

Tailgating: entering an area without authorization verification by following someone who has access.

Uninterruptable Power Supply: an electrical apparatus that provides emergency power to a load when the input power source, typically mains power,

1. Preamble

Data Centers are found in almost all organizations. These data centers host the server environment and electronic data. Due to the sensitivity nature of these data centers, a policy is imperative to guide the Department on the proper mechanisms to manage this room as well to protect information

2. Purpose and objectives

The purpose of this document is to provide guidelines and procedures relating to access control, environmental control, and operations of CoGHSTA ICT Data Centre.

3. Scope of Application

This policy is applicable to CoGHSTA employees granted privilege access to Data Centre and cabinet rooms, service providers and consultants, and any other entity.

4. Legal Framework

4.1. State Information Technology Agency act (Act no 88 of 1998)
4.2. Protection of Information Act (Act no 84 of 1982)
4.3. Minimum Information Security Standards (MISS), Second Edition March 1998
4.4. Departmental ICT Security Policy
4.5. Departmental Disaster Recovery Plan

5. Policy Content

5.1 Background

5.1.1. The vulnerability of business critical information systems and the data they contain within the Data Centre makes the site a high value asset, which requires a high degree of protection.

5.1.2. A range of security measures are therefore in place to protect employees, information and physical assets, along with the reputation of CoGHSTA and interested third parties with equipment in the Data Centre.

5.2 Entry Systems and Access Control

5.2.1. Access shall be controlled via Biometrics fingerprint system and all doors shall be fitted with sensors to detect unauthorized or prolonged opening.

5.2.2. Staff and visitors shall not adjust or otherwise tamper with door fittings. Any suspected faults with doors, lights or any security equipment should be reported to Security Services and/or IT Manager immediately.

5.2.3. Any person requiring access to the Data Centre shall sign the log book located within the upper ground security reception area upon arrival.

5.2.4. Only authorised IT and Security Services personnel shall have access to the Data Centre via the biometrics system. Any other personnel including full time employees, contractors and vendors shall be escorted by authorised IT and/or Security personnel during office hours.

5.2.5. Tailgating into restricted areas is prohibited. Care shall therefore be taken by all authorised staff to prevent these. During deliveries, authorised staff shall supervise such work at all times.

5.3. Contractor Access after hours

5.3.1. Security Services shall be responsible for access control and security of the Data Centre outside normal working hours.

5.3.2. In case where contractors require access to Data Centre after hours, Security Services shall be responsible to provide such access and protection.

5.3.3. The IT Manager will authorize the use and changes to be made in the Data Centre.

5.4. Close circuit television

5.4.1. Internal, entry and exits area of the Data Centre shall be monitored by a closed circuit television (CCTV) to capture all Data Centre activities.

5.4.2. CCTV shall be integrated and monitored by Security Services.

6. Safety

6.1. Overview

In addition to the safety precautions outlined herein, the Data Centre safety precautions shall be applied in conjunction with CoGHSTA Occupational Health and Safety policy.

6.2 Signs and Information

6.2.1. Safety signs and information shall be posted at access points to the Data Centre and cabinet rooms.

6.2.2. General notices shall also be posted around the Data Centre providing detailed information on first aid, emergency contacts and general Health and Safety issues.

6.3. Health and safety Considerations

6.3.1. No one should attempt to lift heavy equipment without suitable help.

6.3.2. No one should attempt to lift equipment in and out of racks unaided, particularly where height makes the task more dangerous.

6.3.3. Ear defenders shall be made available and be worn if working in the Data Centre for periods longer than 30 minutes.

6.3.4. Anyone working in the Data Centre for prolonged periods should let staff know of their presence. Users are advised to take regular breaks from working to avoid adverse effects from temperature and noise levels in particular.

6.3.5. Flexible safety barriers shall be available and be used to lift up raised floor tiles.

6.4. Emergency Exits and Fire Alarm Procedures

6.4.1. When the fire alarm is triggered at the Data Centre, normal emergency procedures shall be followed as stipulated by CoGHSTA emergency evacuation procedures. Lifts shall not be used, only emergency stair ways shall be used.

6.5. Fire Detection and Fire Extinguishers

6.5.1. Fire and smoke detection system shall be fitted and linked to audible and virtual alarms.

6.5.2. If an alarm is activated the Data Centre shall be evacuated immediately to avoid gas inhalation and the incident shall be reported to Security Services and IT Manager.

6.6. Electrical Safety

6.6.1. Only qualified electrical technicians shall have access to electrical systems, IT staff and other personnel should contact the relevant electrical personnel when encountering electricity problems.

6.6.2. Request shall be authorised by the IT Manager.

7. Data Centre Use

7.1 Hours of Operation

7.1.1. The Data Centre will be operated during office hours to authorised personnel between 7:30 am to 16:30 pm.

7.1.2. Access afterhours for maintenance purposes will be authorised and delegated by the IT Infrastructure Manager.

7.2 Equipment delivery

7.2.1. Delivery of equipment shall be supervised by authorised personnel upon approval by the Senior Manager: IT

7.3. Control of Equipment

7.3.1. No unused equipment and spares shall be left at the Data Centre.

7.3.2. Alternate storage facility shall be available for such purpose.

7.4. Prohibited Items

The following items are prohibited from the Data Centre:

7.4.1. Combustible materials such as paper and cardboard (except reference manuals as needed).

7.4.2. Food and drink.

7.4.3. Tobacco products.

7.4.4. Explosives and weapons.

7.4.5. Hazardous materials.

7.4.6. Alcohol, illegal drugs and other intoxicants.

7.4.7. Electro-magnetic devices that could cause interference with computer and telecom equipment.

7.4.8. Radioactive materials.

7.4.9. Photographic or recording equipment (other than backup media).

7.5. Cables and Wiring

7.5.1. Cables and wires shall be structured and labelled when running under the raised floor, wall, and equipment racks.

8. Environment

8.1. Air Conditioning

8.1.1. Under floor air conditioning shall be provided in the Data Centre. It shall deliver enough cooling per rack in accordance with design specification.

8.1.2. Service shall be done at least three times a year by a reputable maintenance service provider for Air dale equipment. Certificate for maintenance performed shall be submitted to the Department.

8.2. CO_2 Fire Extinguisher

8.2.1. Under floor air conditioning shall be provided in the Data Centre. It shall deliver enough cooling per rack in accordance with design specification.

8.2.2. Service shall be done at least annually by a reputable maintenance service provider for C02 gas shall be done. Certificate for maintenance performed shall be submitted to the Department.

8.3. Power and Lighting Provisioning

8.3.1. Two single phase power sockets shall be available in each rack and shall be fed directly from the main switch.

8.3.2. Adequate power light shall be available to ensure that all equipment in the Data Centre are clearly visible.

8.3.3. Lights shall be switched off when no access to the Data Centre is required.

8.4. UPS Provisioning

8.4.1. All major equipment at the Data Centre shall be powered on by a UPS system, should the AC power goes down. The UPS system should sustain power to those devices for at least 5 minutes to allow graceful shutdown.

8.4.2. Service shall be done at least annually by a reputable maintenance service provider for APC Galaxy equipment. Certificate for maintenance performed shall be submitted to the Department.

8.5. Temperature and Humidity

8.5.1. Temperature and Humidity monitoring devices shall be implemented and set to monitor deviations against baseline set according to standard recommended by GITO.

8.6. Environment Monitoring

A number of monitors shall be put in place to report on issues affecting the Data Centre environment. Monitoring system shall report to designated IT and Security personnel, monitoring shall include:

8.6.1. Temperature and Humidity alarms.
8.6.2. Fire and Smoke Detectors.
8.6.3. UPS malfunctioning or discharge during normal AC power operation.
8.6.4. Daily monitoring.

8.7. Dust Prevention

8.7.1. The Data Centre shall be well ventilated to prevent dust from affecting equipment.
8.7.2. Equipment to be installed in the Data Centre shall be dust freed outside before introduced.

8.8. Waste Disposal and Cleaning

8.8.1. Cardboard and other items that can generate dust and that are easily combustible should remain outside the Data Centre.
8.8.2. Waste bin shall be available outside the Data Centre main entrance for easy disposal of other items of waste.

8.9. Change and Configuration Management

8.9.1. The IT Manager is responsible for all changes that shall take place at the Data Centre.
8.9.2. All changes to be made shall be requested to and authorised by the IT Manager.
8.9.3. The IT Manager will monitor and review the Data Centre access log book on a regular basis.

9. Administration of the Policy

9.1. GITO/CFO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

10. Policy Review

This policy shall be reviewed Bi-annually.

11. Default

Non-compliance of this policy shall constitute violation of the policy and shall be treated in terms of the departmental disciplinary code and procedure policy.

12. Inception Date

This policy comes into effect from the date of approval by Member of Executive Council.

13. Enquiries

Enquiries about the policy should be directed to the Government Information Technology Office.

Document Title	**ICT Data Centre Physical Access and Environmental Control Policy**
Compiled by :	**Government Information Technology Office**  **Senior Manager** **(ICT Infrastructure and Systems)** 18/12/2014 **Date**
Acknowledge by :	 **General Manager (GITO)** Acting 18/12/2014 **Date**
Qualified by:	 **Senior Manager** **(Research and Policy Coordination)** 23/12/2014 **Date**
Recommended by:	 **Senior General Manager** **(Corporate Services)** 05th/01/2015 **Date**
Adopted by :	 **Head of Department** 07/01/2015 **Date**
Approved by :	 **Member of the Executive Council** 07/01/2015 **Date**