LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

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

ICT Data Centre Physical Access and Environmental Control Policy

Date: 20 February 2012

Version: 1

Version Control

Version	Date	Author(s)	Details
Draft 1.0	06/01/2012	Samuel Mantlaka	Draft Data Centre Physical Access and Environmental Control Policy
Final	27/02/2012		Adopted by Labour Management Forum

Contents

1.   Preamble

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

2.   Definitions

Access Control: Mechanisms and policies that restrict access to resources

AC: 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

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

COGHSTA: Department of Co-operative Governance, Human Settlements and Traditional Affairs

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: Types of floor that provide an elevated structural floor 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 authorisation verification by following someone who has access

UPS: an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails

3.   Purpose

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

4.   Scope

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

5. Legal Framework

State Information Technology Agency Act (Act no 88 of 1998)
Protection of Information Act (Act no 84 of 1982)
Minimum Information Security Standards (MISS), Second Edition March 1998
Departmental ICT Security Policy
Departmental Disaster Recovery Plan
Departmental Occupational Health and Safety policy

6. Policy Content

6.1 Background

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

6.2 Entry Systems and Access Control

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

6.2.2. 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.

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

6.2.4. 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 will be escorted by authorised IT and/or Security personnel during office hours.

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

6.3 Contractor Access after hours

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

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

6.3.3   The IT Manager will authorise the use and changes to be made in the Data Centre.

6.4   Close circuit television

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

6.4.2   CCTV shall be integrated and monitored by Security Services.

7.   Safety

7.1   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.

7.2   Signs and information

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

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

7.3   Health and Safety Considerations

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

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

7.3.3   Noise levels shall be checked at every half-year to ensure a safe working environment.

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

7.3.5   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.

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

7.4 Emergency Exits and Fire Alarm Procedures

7.4.1 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.

7.5 Fire Detection and Fire Extinguishers

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

7.5.2 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.

7.6 Electrical Safety

7.6.1 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.

7.6.2 Request shall be authorised by the IT Manager.

8. Data Centre Use

8.1 Hours of Operation

The Data Centre will be operated during office hours to authorised personnel between 7:30 am to 16:30 pm.
Access afterhours for maintenance purposes will be authorised and delegated by the IT Manager.

8.2 Equipment Delivery

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

8.3 Control of Equipment and Spares

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

8.3.2   Alternate storage facility shall be available for such purpose.

8.4   Prohibited Items

The following items are prohibited from the Data Centre:

8.4.1.   Combustible materials such as paper and cardboard (except reference manuals as needed)
8.4.2.   Food and drink
8.4.3.   Tobacco products
8.4.4.   Explosives and weapons
8.4.5.   Hazardous materials
8.4.6.   Alcohol, illegal drugs and other intoxicants
8.4.7.   Electro-magnetic devices that could cause interference with computer and telecom equipment
8.4.8.   Radioactive materials
8.4.9.   Photographic or recording equipment (other than backup media).

8.5   Cables and Wiring

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

9.   Environment

9.1   Air Conditioning

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

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

9.2   CO2 Fire Extinguisher

9.2.1   Class E gas fire extinguisher shall be implemented to prevent damage to Data Centre electrical facilities.

9.2.2   Service shall be done at least annually by a reputable maintenance service provider for CO_2 gas shall be done. Certificate for maintenance performed shall be submitted to the Department.

9.3 Power and lighting Provisioning

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

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

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

9.4 UPS Provisioning

9.4.1 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.

9.4.2 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.

9.5 Temperature and Humidity

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

9.6 Environment Monitoring

9.6.1 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

9.6.2 Monitoring shall include:

9.6.3 Temperature and Humidity alarms

9.6.4 Fire and Smoke Detectors

9.6.5 UPS malfunctioning or discharge during normal AC power operation and

9.6.6 Daily monitoring.

9.6.7   Service shall be done biannually by a reputable maintenance service provider for EnviroCabinets equipment. Certificate for maintenance performed shall be submitted to the Department.

9.7   Dust Prevention

9.7.1   The Data Centre shall be well ventilated to prevent dust from affecting equipments.

9.7.2   Equipment to be installed in the Data Centre shall be dust freed outside before introduced into the Data Centre.

9.8.   Waste Disposal and Cleaning

9.8.1   Cardboard and other items that can generate dust and that are easily combustible should remain outside the Data Centre.

9.8.2   Waste bin shall be available outside the Data Centre main entrance for easy disposal of other items of waste.

9. 9   Change and Configuration Management

9.9.1   The IT Manager is responsible for all changes that shall take place at the Data Centre

9.9.2   All changes to be made shall be requested to and authorised by the IT Manager.

9.9.3   The IT Manager will monitor and review the Data Centre access log book on a regular basis.

10.   Procedure of Non-Compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.

11.   Policy Review

This policy shall be reviewed annually.

12.   Effective Date

This policy comes into effect from the date of approval.

COMPILED BY--

SENIOR MANAGER: 06/03/2012
                                                             DATE
INFORMATION TECHNOLOGY

ACKNOWLEDGED BY:

Adoption and approval of ICT Data Centre
Physical access and environmental control
policy is recommended.

GENERAL MANAGER: 06/03/2012.
                                                             DATE
GOVERNMENT INFORMATION TECHNOLOGY OFFICE

ACKNOWLEDGED BY:
                Supported for approval.

U Manael   08/03/2012
SENIOR GENERAL MANAGER: DATE

SHARED SERVICES

ADOPTED /NOT ADOPTED:
                Supported

U Manael   08/03/2012
HEAD OF DEPARTMENT   DATE

APPROVED/~~NOT APPROVED~~

_____   28/03/12

HONOURABLE MEC   **DATE**