



IT-05-24

ICT Data Centre Physical Access and Environmental Control Policy

Document Name: ICT Data Centre Physical
Access and Environmental
Control Policy

Policy Number: ICT-011

Version: 003

Date Issued: May 2024

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	1

Document Information

Policy	ICT Data Centre Physical Access and Environmental Control Policy
Version	003
Policy Code	ICT-011
File Name	POL-ICT-05-24 Data centre.doc
Date Issued	May 2024
Policy Enforcer	ICT Manager

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	2

Table of Contents

I.	Acronyms and Abbreviations.....	4
II.	Definitions.....	5
1.	Preamble.....	6
2.	Purpose and objectives.....	6
3.	Scope of Application	6
4.	Legal Framework	6
5.	Administration of the policy	7
6.	Policy Statement	7
7.	Entry Systems and Access Control.....	7
8.	Contractor Access after hours.....	8
9.	Close circuit television.....	8
10.	Safety	8
11.	Data Centre Use	10
12.	Environment.....	11
13.	Inception Date	14
14.	Policy Review.....	14
15.	Enquiries	14

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	3

I. Acronyms and Abbreviations

4G	Fourth Generation
ICT SBU	Information Communication Technology Sub Business Unit
ICT Manager	Information Communication Technology Manager
VPN	Virtual Private Network
AC	Alternating Current
UPS	Uninterrupted Power Supply
CCTV	Closed Circuit Television

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	4

II. 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

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

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	5

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 Municipality 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 Polokwane Municipality ICT Data Centre.

3. Scope of Application

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

4. Legal Framework

The following publications govern the execution of the Data Centre Physical Access and Environmental Control Policy and were taken into consideration during the compilation of the policy:

4.1. Protection of Information Act (Act no 84 of 1982)

4.2. Protection of Personal Information Act (Act no 4 of 2013)

4.3. Minimum Information Security Standards (MISS), Second Edition March 1998

4.4. Municipal ICT Security Policy

4.5. Municipal Disaster Recovery Plan

4.6. Municipal Occupational Health and Safety policy

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	6

4.7. Municipal ICT Equipment Usage Policy.

5. Administration of the policy

ICT Manager is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. Policy Statement

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 Polokwane Municipality and interested third parties with equipment in the Data Centre.

7. Entry Systems and Access Control

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

7.2. Staff and visitors should 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 ICT Manager immediately.

7.3. Any person requiring access to the Data Centre shall sign the Data Centre access register located in the server room upon arrival.

7.4. Only authorised ICT 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 ICT and/or Security personnel at all times.

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	7

7.5. 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.

8. Contractor Access after hours

8.1. Security Services shall be responsible for access control and security of the Data Centre at all times.

8.2. In case where contractors require access to Data Centre after hours, ICT staff shall be responsible to provide such access and be accompanied by Security services personnel.

8.3. The ICT Manager will authorise the use and changes to be made in the Data Centre.

9. Close circuit television

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

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

10. Safety

10.1. Overview

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

10.2. Signs and information

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	8

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

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

10.3. Health and Safety Considerations

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

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

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

10.3.4 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.

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

10.4. Emergency Exits and Fire Alarm Procedures

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

10.5. Fire Detection and Fire Extinguishers

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

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	9

10.5.2 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 ICT Manager.

10.6. Electrical Safety

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

10.6.2 Request shall be authorised by the ICT Manager.

11. Data Centre Use

11.1. Hours of Operation

11.1.1 The Data Centre shall be operated during office hours by authorised personnel between 7:45 am to 16:30 pm.

11.1.2 Access for maintenance purposes after hours shall be authorised and delegated by the ICT Manager.

11.2. Equipment Delivery

11.2.1 Delivery of equipment shall be supervised by authorised personnel upon approval by the ICT Manager.

11.3. Control of Equipment and Spares

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

11.3.2 Alternate storage facility shall be available for such purpose.

11.4. Prohibited Items

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	10

The following items are prohibited from the Data Centre:

- 11.4.1 Combustible materials such as paper and cardboard (except reference manuals as needed)
- 11.4.2 Food and drinks
- 11.4.3 Tobacco products
- 11.4.4 Explosives and weapons
- 11.4.5 Hazardous materials
- 11.4.6 Alcohol, illegal drugs and other intoxicants
- 11.4.7 Electro-magnetic devices that could cause interference with computer and telecom equipment
- 11.4.8 Radioactive materials
- 11.4.9 Photographic or recording equipment (other than backup media).

11.5. Cables and Wiring

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

12. Environment

12.1. Air Conditioning

- 12.1.1 Under floor air conditioning shall be provided in the Data Centre. It shall deliver enough cooling per rack in accordance with design specification.
- 12.1.2 Service shall be done at least quarterly by a reputable maintenance service provider for cooling equipment. Certificate for maintenance performed shall be submitted to the Municipality.

12.2. CO2 Fire Extinguisher

Class E gas fire extinguisher shall be implemented to prevent damage to Data Centre electrical facilities. Service shall be done at least annually by a reputable maintenance

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	11

service provider for CO₂ gas shall be done. Certificate for maintenance performed shall be submitted to the Municipality.

12.3. Power and lighting Provisioning

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

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

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

12.4. UPS Provisioning

12.4.1 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.

12.4.2 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 Municipality.

12.5. Temperature and Humidity

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

12.6. Environment Monitoring

12.6.1 A number of monitors shall be put in place to report on issues affecting the Data Centre environment. Monitoring system shall report to designated ICT and Security personnel

12.6.2 Monitoring shall include:

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	12

- a) Temperature and Humidity alarms
- b) Fire and Smoke Detectors
- c) UPS malfunctioning or discharge during normal AC power operation and
- d) Daily monitoring.
- e) Service shall be done biannually by a reputable maintenance service provider. Certificate for maintenance performed shall be submitted to the Municipality.

12.7. Dust Prevention

12.7.1 The Data Centre shall be well ventilated to prevent dust from affecting equipment.

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

12.8. Waste Disposal and Cleaning

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

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

12.9. Change and Configuration Management

12.9.1 The ICT Manager is responsible for all changes that shall take place at the Data Centre

12.9.2 All changes to be made shall be requested to and authorised by the ICT Manager.

12.9.3 The ICT Manager will monitor and review the Data Centre access register on a regular basis.

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	13

13. Inception Date

This policy comes into effect from the date of approval.

14. Policy Review

This policy shall be reviewed every three (3) years.

15. Enquiries

Enquiries about the policy should be directed to the ICT Manager.

* * *

<i>Policy:</i>	ICT Data Centre Physical Access and Environmental Control Policy	<i>Policy Code:</i>	ICT-011
<i>Version:</i>	003	<i>Date Issued:</i>	May 2024
		<i>Page</i>	14