



GAUTENG PROVINCE

HEALTH
REPUBLIC OF SOUTH AFRICA

ICT SERVER ROOM AND DATA CENTER ENVIRONMENT POLICY

DEVELOPING CHIEF DIRECTORATE: ICT

APPROVAL DATE:

REVIEW DATE:

HOD's FOREWORD

The Gauteng Department of Health manages, advises and provides oversight for Server Rooms and Data Centres at all its facilities. In order to ensure compliance and commitment to standardization, it is imperative that a policy governing the server rooms / data centres be instituted.

The Server Room and Data Centre Policy and its implementation processes emphasises globally endorsed values and required compliance to ensure continual and uninterrupted service rendition with respect to services hosted and supported by the ICT component. The policy will cover and endorse environmental management, access control and power management. The institution of this policy will serve to ensure sustainable and professional services to ensure availability of services across all facilities.

Systems, software and ICT services form an integral part of ensuring that the Gauteng Department of Health provides a platform of services that not only assist its staff complement in professionally rendering their job functions, but also enabling the population of Gauteng to benefit from such services. This policy will serve to ensure that these attributes are adhered to.

The policy will require that all affected personnel comply with and efficiently practise the recommendations of the policy to ensure that the Gauteng Department of Health is able to successfully provide an infrastructure inclined toward ensuring service excellence.

Mr. L. A. Malotana

Acting Head of Department

Date:

Contents

1. DEFINITION OF TERMS AND ACRONYMS	4
1.1. Terms.....	4
1.2. Acronyms	4
2. INTRODUCTION	5
3. POLICY OBJECTIVES	5
4. SCOPE OF THE POLICY	5
5. PROBLEM STATEMENT	5
6. LEGISLATIVE FRAMEWORK.....	6
7. CONSULTATION.....	6
8. POLICY IMPLEMENTATION.....	7
8.1. Policy Interventions	7
8.1.1. Entry Systems and Access Control	7
8.1.2. CCTV	7
8.1.3. Safety.....	7
8.1.4. Data Centre Use	8
8.1.5. Prohibited Items	9
8.1.6. Cables and Wiring	9
8.1.7. Environment	9
8.2. Roles and Responsibilities	11
8.2.1. Server Administrators (ICT Head Office)	11
8.2.2. IT Managers (ICT Institution)	12
8.2.3. Users of server rooms/ data centres	13
8.2.4. Contractor Access after hours	13
8.3. Resource Requirements.....	13
8.4. Training Plan	13
9. POLICY MONITORING	14
9.1. Policy Outputs	14
Reduced damages, theft and losses of equipment and enviromentals	14
9.2. Monitoring Mechanisms.....	14
9.3. Compliance.....	14
10. REVIEW	14
11. APPROVAL	15

1. DEFINITION OF TERMS AND ACRONYMS

1.1. Terms

Access Control	Mechanisms and policies that control access to resources; in this instance, access to the Server Room
Alternating Current	An electric current that frequently reverses direction
Biometrics	Process by which a person's unique physical and other traits are detected
Closed Circuit Television	The use of video cameras to transmit a signal / image to a identified collative server environment
Server Room/ Data Centre	Facility used to house computer systems and associated components, namely – telecommunication, storage, network and other systems. The server room usually includes redundant or back-up power suppliers, redundant data communication systems, environmental controls such as cooling equipment and fire suppression, etc....), and security devices
Fire Extinguishers	An active protection device used to extinguish or control small outbreak of fire, usually in an emergency situation
Raised flooring	Set of grind-locked fire proof tiles that resides on an elevated framework above the normal substrate (usually concrete), for the purpose of hidden reticulation of mechanical and electrical services
Tailgating	Garnering entry into an area without permission, authorization or verification by closely following someone who has already entered via authorization
Uninterrupted Power Supply (UPS)	A mechanical device that ensure temporary emergency power supply to connect equipment during period of power supply interruption
Cooling System	A functional cooling system that will operation within specified temperatures, to ensure continual functioning of all equipment in the server room. It could be HVAC or split units.
Cable Trays	A dedicate cables channel to host and protect cables and separate between power & data cables.

1.2. Acronyms

Acronym	Definition
AC	Alternating Current
GDoH	Gauteng Department of Health
HOD	Head of Department
MEC	Member of Executive Council
UPS	Uninterruptable Power Supply
ICT	Information and Communication Technology Chief Directorate
SMS	Senior Management Services
SOP	Standard Operating Procedure
DRP	Disaster Recovery Plan
OHS	Occupational Health and Safety
CO2	Carbon Dioxide
CCTV	Closed Circuit Television
HVAC	Heating, Ventilation and air conditioning

2. INTRODUCTION

The server room is the brain of GDoH IT infrastructure. It houses the servers, switches, routers, storage devices, and other critical equipment that run the departmental business. However, server rooms are prone to various problems that can cause downtime, data loss, and other costly consequences.

Server room is a room used to put network devices and server computers that contain important and valuable data for the any department that already implement IT technology in its operational activities. Server room should always be monitored at all times.

The department is currently using the physical management policy approved in 2011, to manage the server rooms/data centres. The existing policy does not provide processes for entry and access control, contractors after hours, safety, cables and wiring. As a result, there is no consistency in the usage and management of the server room/ data centre.

3. POLICY OBJECTIVES

The objectives of the policy are to:

- To ensure alignment of Departmental policies with internationally accepted models / trends;
- To ensure compliance and standardization of the utilization of the data centre / server room.

4. SCOPE OF THE POLICY

The policy applies to all permanent and contracted employees of the Department and other users of server rooms / data centres. The policy applies to all server rooms owned but have access to the corporate network, data and systems. This includes any cooling, electrical safety, and cables.

5. PROBLEM STATEMENT

The Gauteng Department of Health (GDOH) Information Communication Technology (ICT) still have servers in our institutions that hold departmental information. There are

more users dependent upon the server room / data centres for communication purposes and to perform health services to meet the mandate of the department.

There is currently no standard governing server room / data centres within the province, and this will lead to non-compliance in terms of industry wide standards. Adoption of the proposed new policy will address professional and compliant utilization of the data centre / server room. Non-compliance of these aspects may and will result in compromised control measures.

The current departmental policy has lapsed and is not aligned with the National and International standards. The current policy does not align to contemporary trends in data centre management and further does not provide sufficient control measures with respect to access control and environmental management. There is also abuse in terms of using server rooms/data centres. How to access the server rooms/data centre is not articulated in the current policy.

6. LEGISLATIVE FRAMEWORK

This policy is informed by the following prescripts:

- Public Finance Management Act, Act 1 of 1999 (As Amended);
- Cost Containment Instruction Note 2 of 2016/2017;
- Labour Relation Act, Act 66 of 1995
- State Information Technology Act (Act 8 no. 88 of 1998)
- Protection of Information Act (Act no. 84 of 1982)
- Minimum Information Security Standard (MISS), 2nd Edition March 1998

7. CONSULTATION

The following stakeholders were invited to provide inputs on the draft policy:

- Executive Management Technical Committee
- ICT Managers; and
- Policy Development and Review Committee

8. POLICY IMPLEMENTATION

8.1. Policy Interventions

- By aligning with the international accepted models/trends
- By providing procedures and processes to access the server room/ data centre.

8.1.1. Entry Systems and Access Control

- a) Access to server rooms/data centres shall be controlled via the usage of an access card (current) / or a biometric fingerprint system (future) and all doors shall be fitted with sensors to detect unauthorized or prolonged opening;
- b) Staff and visitors shall not adjust or otherwise tamper with door fittings. Any suspected faults with doors, light or any security equipment shall be reported to Security Services and / or the IT Managers responsible immediately;
- c) Any person requiring access to the server room shall sign the register/ log book located with the responsible IT Manager upon arrival (and only if prior arrangement has been made;
- d) Only authorized ICT and Security Services personnel shall have access to the server room via the biometric / card system. Any other person, including full time employees, contractors and vendors shall be escorted by an authorized ICT personnel or Security service personnel during office / after hours;
- e) Tailgating into the server room is strictly prohibited. Care shall be taken by all authorized staff to prevent such entry;
- f) Authorized staff shall supervise and monitor deliveries at all times.

8.1.2. CCTV

- a) Entry, exit and internal areas of the server room shall be monitored by the CCTV deployment to capture all activities in and around the server room.
- b) The CCTV shall be integrated with and monitored by security services.

8.1.3. Safety

- a) Safety precautions relating to the server room /data centre outlined herein, shall be applied in conjunction with the GDoH's OHS policy.

- b) Safety signs and information shall be posted at access points to the server room /data centre at all facilities.
- c) General notices shall be posted around the server room providing detailed information on first aid, emergency contacts and general health and safety measures.
- d) No one shall attempt to lift heavy equipment without suitable help.
- e) No one shall attempt to lift equipment in and out of racks unaided, and particularly where the height makes the task more dangerous.
- f) Anyone working in the data centre for prolonged periods shall let other staff members know of their presence. Users shall take regular breaks to avoid adverse effects from reduced temperatures levels and increased noised levels in particular.
- g) Proper tile lifters must be made available to lift tiles when required.
- h) Flexible safety barriers must be available when tiles have been lifted for extended period of time.
- i) Lifts shall not be used when an alarm is triggered at the server room, only identified staNormal emergency procedures shall be followed as stipulated by the GDoH emergency evacuation procedure only emergency stairways shall be used in case of emergency.
- j) Fire and smoke detection systems shall be fitted and linked to audible and visible alarms.
- k) If an alarm is activated, the server room shall be immediately evacuated to avoid gas inhalation and the incident shall be reported to security services and the relevant IT manager; Safety incidents must also be reported to the Department of Labour, as stipulated in Section 24 of the Occupational Health and Safety Act. The OHS Unit must be consulted on this policy to ensure that there are no policy contradictions and role confusion.
- l) Only qualified electrical technicians shall have access to the electrical systems. Technicians must be contacted during any electrical problem/ occurrence; request for this service must be made by IT manager.

8.1.4. Data Centre Use

- a) The server room/ data centre shall be available to authorized personnel between 07:30 am and 16:30 pm.
- b) Access to the server room/data centre after hours and/or for maintenance purposes shall be authorized by the delegated the IT Manager.

- c) Delivery of equipment shall be supervised by authorized personnel upon approval of the IT Manager.
- d) No unused equipment and spares shall be left within the confines of the server room.
- e) Alternate storage must be provided for unused equipment.

8.1.5. Prohibited Items

The following items are prohibited from the server room:

- a) Combustible material such as paper and cardboard (except for reference manuals, as required);
- b) Food and drinks
- c) Tobacco products
- d) Explosives and weapons
- e) Hazardous materials
- f) Alcohol, illegal drugs and other intoxicants
- g) Electro-magnetic devices that can interfere with computer and/or telecommunications devices
- h) Radio-active material
- i) Photographic or recording equipment (other than back-up media).

8.1.6. Cables and Wiring

- a) Cables and wires shall be structured and labelled, whether running under floor, along walls, in equipment racks or overhead

8.1.7. Environment

8.1.7.1 Air conditioning/ cooling

- a) Under floor air conditioning shall be implemented within the data centre, and must be designed to provide sufficient cooling capacity per rack, as per the required specifications;
- b) Servicing shall be performed at least three times per year by a reputable/ certified service provider. Certificates for such work shall be lodged with GDoH;

- c) A contract with a minimum 3 -5 year maintenance plan shall be in place to ensure such a service.

8.1.7.2 CO2 Fire Extinguisher

- a) A CO2 fire suppressant system must be installed to mitigate any fire disaster;
- b) This system must be serviced at a minimum, annually, by a certified service provider. Certificates of service must be lodged with GDoH facilities management unit or ICT.

8.1.7.3 Power and lighting provisioning

- a) A 3-phase power reticulation must be evident;
- b) Each rack shall be provisioned with a minimum of two 16amp caravan plugs fed directly from the main distribution board;
- c) Sufficient electrically powered lighting must be installed to provide clear visibility to all racks and racked equipment;
- d) Lights must be switched off when server room is not in use, unless an automated green system has been installed.

8.1.7.4 UPS provisioning

- a) All major equipment in the server room must receive power via an UPS reticulation. The UPS must be capacitated to provide a minimum of 5 minutes to allow for graceful shutdown of all equipment;
- b) UPS unit must be serviced at least annually by a certified installer/ supplier and certificate of maintenance must be lodged with GDoH facilities management unit.
- c) In the event of a power generator system, all power entering server room must be reticulated via the UPS to ensure protection from surges, brown-outs, etc.

8.1.7.5 Temperature and humidity

- a) Temperature and humidity monitoring/detecting devices shall be implemented and set to monitor deviations against an identified baseline recommended by industry standards.

8.1.7.6 Environment Monitoring

- a) Monitors shall be in place to ensure reporting on issues arising within the server room. The monitoring system will emit warning reports to IT manager and Security services. Monitoring shall include:
- b) Temperature and humidity alarms;
- c) Fire and smoke detectors;
- d) UPS Malfunctioning or abnormal discharge;
- e) Daily monitoring.

8.1.7.7 Dust prevention

- a) The server room shall be well ventilated in order to prevent dust pollution;
- b) Equipment to be installed must be rendered dust free (outside server room) before installation takes place

8.1.7.8 Waste disposal and cleaning

- a) Cardboard, paper and other items that can regenerate dust or pose a fire hazard shall remain outside the data centre;
- b) A waste bin shall be located immediately outside the server room for easy disposal of waste items

8.2. Roles and Responsibilities

8.2.1. Server Administrators (ICT Head Office)

- a) Ensure that this policy is enforced and complied with;
- b) Hold and maintain the Access Logs;
- c) Manage in-house computer software systems, servers, storage devices and network connections to ensure high availability and security of the supported business applications;
- d) Have familiarity with MS SQL server, windows clustering, domain controller setup, and group policy;
- e) Recommend, schedule, and perform software and hardware upgrades, patches and reconfigurations;

- f) Ensure the security of the server infrastructure by implementing industry best-practices regarding privacy, security, and regulatory compliance;
- g) Develop and maintain documentation about current environment setup, standard operating procedures, and best practices;
- h) Manage end user accounts, permissions, access rights, and storage allocations in accordance with best practices;
- i) Perform and test routine system backups and restores;
- j) Anticipate, mitigate, identify, troubleshoot, and correct hardware and software issues on servers, and workstations. Escalate incidents as necessary;
- k) Practice server asset management, including maintenance of server component inventory, related documentation and technical specifications information;
- l) Develop required reports in response to business users and management needs;
- m) Manage vendors, outsourcers, and contractors to secure software products and services;
- n) Manage the physical environment of the server racks including cable management, documentation, labeling, and configuration of switching for console and remote access;
- o) Build and deploy new servers on the network as needed.

8.2.2. IT Managers (ICT Institution)

- a) Maintains quality service by establishing and enforcing organizational standards.
- b) Ensures that this policy is enforced and complied with;
- c) Holding and maintaining the Access Log.
- d) Performs basic server administration and general data centre maintenance.
- e) Made visitors aware of this policy and their obligations therein. Accompany visitors to ensure that they carry out their duties in a professional manner whilst working in the IT Server rooms/Data Centre.

8.2.3. Users of server rooms/ data centres

- a) All other staff members with rights to access must be aware of this policy and their obligations therein. It is their responsibility to ensure they carry out their duties in a professional manner whilst working in the IT Server Rooms/ Data Centres
- b) Staff must always wear their identification badge.
- c) All individuals accessing the IT Server Rooms must sign in and out of the IT Server Rooms Access Log. This includes all visitors, who must be always accompanied by a member of the IT staff.

8.2.4. Contractor Access after hours

- a) Security services shall be responsible for access control and security of the server room outside normal working hours. This can also be borne by authorized personnel if proper and prior arrangements have been made;
- b) In case where contractors require access to the server room after hours without prior arrangement, the security services shall call the responsible IT Manager for authorization, and thereafter provide access and protection;
- c) The responsible IT Manager shall always authorize the use of and changes to be made in the server room.

8.3. Resource Requirements

Additional human resources will be needed for server administration purposes at the institutional level.

8.4. Training Plan

Training on the policy shall be provided to all server administrators within three months after the approval of the policy.

9. POLICY MONITORING

9.1. Policy Outputs

Output	Performance measures	Timelines
Reduced damages, theft and losses of equipment and enviromentals	Number of damages, theft and losses incident reports	Ongoing
Reduced incidents of unauthorized access to server rooms	Number of unauthorized users identified	Ongoing

9.2. Monitoring Mechanisms

The ICT Directorate shall monitor the implementation of the policy through holding monthly meetings with ICT Managers to obtain feedback on the implementation of the policy. ICT Managers shall submit monthly reports on the implementation of the policy to the Server Administration Manager.

The Server Administrators shall submit monthly reports to Head office ICT Infrastructure Server Manager for monitoring purposes.

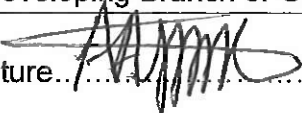
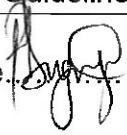
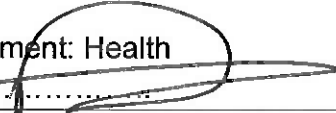
9.3. Compliance

Ongoing training on Server Room Policy shall be provided to ensure compliance. Failure to comply with the with the provisions of the Server room Policy may result in disciplinary action.

10. REVIEW

The policy shall be reviewed every three (3) years or as and when a need arises.

11. APPROVAL

FOR OFFICE USE ONLY	
THE KEY STAKEHOLDERS CONSULTATION	
Policy written by: ANELE APLENI	
The developing Branch or Chief Directorate acknowledges and accepts the policy	
Signature..... 	Date.....17/04/2024
Comment.....	
Technical support provided by CD: Policy, Planning, Research and HIEM	
Assurance that technical support was given, and Policy Development, Review and Approval Guidelines followed	
Signature..... 	Date.....09/05/2024
Comments.....	
APPROVAL OF POLICY	
Approved/Not Approved/Approved with Amendments	
The HOD approves operational policies	
Head of Department: Health Signature..... 	Date.....20/05/17
Comments: 