

1. POLICY TITLE

ICT Infrastructure Management and Maintenance Policy

2. PREAMBLE

The Langeberg Municipality ICT infrastructure is made up of different pieces of equipment, ranging as follows: firewalls, routers, switches, servers, storage, desktop PCs, laptops, printers, etc. All this equipment, amongst others, are part of the Langeberg network ensures communication and interconnectivity to each of the devices for ICT service delivery. The main benefit of the interconnected nature of the ICT devices is that it allows centralized management and monitoring of network access and network data, and such devices can have power, hard drive and processor redundancies that are typically not available in any ordinary machine. Performing regular maintenance of ICT infrastructure, with just a little time, yields the most performance and return on investment which significantly extends the shelf life of ICT equipment. All ICT infrastructure can be maintained easily to reduce ICT service interruptions. Hence, this policy provides the Langeberg Municipality with principles of managing the maintenance of the Municipality's ICT environment.

3. LEGAL MANDATES AND REGULATORY FRAMEWORK

The statutory framework on which the ICT Infrastructure Management and Maintenance Policy is founded are the following;

- Electronic Communications and Transactions Act (Act No. 25 of 2002);
- SITA Communications and Network Security Policy International Standards Organization 17799;
- Electronic Communications Act 36 of 2005.

The following internationally recognized ICT standards were leveraged in the development of this policy:

- Control Objectives for Information Technology (COBIT) 5, 2012

-ISO 27002: 2013 Information technology - Security techniques - Code of practice for information security controls

4. PURPOSE OF THE POLICY

The purpose of this policy is:

- To outline the ICT Infrastructure Management Standards.
- To ensure access to key ICT facilities is restricted to individuals who are involved in the operation and maintenance of such facilities and is recorded.

5. STRATEGIC OBJECTIVES

This policy provides the ICT infrastructure and mechanisms to help the organisation realise its goals and objectives in setting ICT infrastructure management standards. Access to server rooms should be justified, authorised, logged and monitored. As such, this document applies to all personnel with access to server rooms, including those entering the premises, together with staff, temporary staff, clients, vendors, visitors or any other third party.

6. POLICY PRINCIPLES

The policy will be based on the COBIT 5 best practice for ICT equipment environmental controls maintenance

7. DEFINITIONS

Policy

A policy statement defines a general commitment, direction, or intention. A policy statement expresses management's commitment to the implementation, maintenance, and improvement of its information security management system.

Control

A control is any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards and/ or counter measures. Controls include practices,

policies, procedures, programs, techniques, technologies, guidelines, and organisational structures. Controls can be deterrent, preventive, protective, detective and corrective.

8. SCOPE OR APPLICABILITY OF THE POLICY

The following key objectives are critical and applicable to the Langeberg ICT infrastructure which all forms the backbone of the network and manages data:

8.1 Operating System

- I. The operating system for all the servers is Windows Server 2019 and Windows Server 2022.
- II. The operating system for all the desktop PCs and laptops is Windows 10 and Windows 11.
- III. The operating system of every server, desktop PC, and laptop will be upgraded every 5 years with the latest patches.
- IV. Testing of the operating system will be conducted on a test environment before deployment to production.

8.2 Hardware

- I. The server hardware manufacturers are Hewlett Packard Enterprise (HPE).
- II. The server hardware will be upgraded every five (5) to seven (7) years.
- III. The desktop PC and laptop hardware manufacturers are HP, Acer, and Dell.
- IV. The desktop PC and laptop hardware will be upgraded every three (3) to five (5) years.
- V. Storage device manufacturers are Netapp with a replacement of upgrade every 5 of 7 years.
- VI. The Uninterrupted Power Supply (UPS) hardware manufacturer is American Power Corporation (APC) with a battery shelf life of 3 to 5 years.
- VII. Office printers in use are Konica Minolta and HP.
- VIII. The network equipment hardware manufacturers are Cisco, Mikrotik, HPE, Ubiquiti, and Dell with a preferred refresh rate of 3 to 5 years.
- IX. CCTV equipment manufacturers are HikVision.

8.3 Security

- I. The firewall manufacturers are SonicWall and Cisco.
- II. The Endpoint anti-virus is Sophos.
- III. Anti-virus updates are deployed on monthly basis on all servers.
- IV. All access to the servers is authenticated with Active Directory.
- V. All the servers are in a domain network which is protected by the network firewall.
- VI. All ICT infrastructure is password-protected and requires authentication for successful access.

8.4 Server Rooms

- I. The server rooms and other rooms which host ICT equipment and hardware are fitted with air-conditioners for temperature control.
- II. There are standby generators which provide backup power in cases of power outages to ICT equipment and hardware.
- III. Server rooms are fitted with biometric devices for access control.
- IV. To ensure fire prevention and control, there are sensors and fire extinguishers installed in the server rooms.

8.5 Data

- I. Electronic data is stored in both on-premise storage devices, such as disks and tapes and in private cloud storage.
- II. Personal, financial, legal, and other business-related data is stored on the storage devices electronically.
- III. The retention of electronic data on the ICT storage systems is maintained to a minimum of seven (7) years.

8.6 Maintenance Plan

- I. Quarterly maintenance will be conducted on all the servers during weekends.
 - a. Backup is first conducted on the servers and storage.
 - b. Servers and storage are patched with latest updates.
 - c. Physical cleaning of the server and storage hardware to remove all the dust.

- d. Health inspection is then conducted on the servers and storage.
 - e. Test if all the applications, systems and files installed or stored on the servers and storage are functional.
 - f. Conduct backup test for the applications, systems and files.
- II. Monthly maintenance will be conducted on the perimeter firewalls during weekends.
 - a. Configuration backup is first conducted on the firewalls.
 - b. Firewalls are patched with latest firmware updates.
 - c. Physical cleaning (blowing) of the firewall hardware to remove all the dust.
 - d. Health inspection is then conducted on the firewall.
 - e. Test if all the configuration rules and parameterization saved on the firewall are functional.
 - f. Conduct backup test for the firmware and configuration.
- III. Ad-hoc maintenance will be conducted on the office printers.
 - a. The print server configuration is backed up when the server is backed up.
 - b. Printers are patched with latest firmware updates.
 - c. Physical cleaning (blowing) of the printer hardware to remove all the dust.
 - d. Health inspection is then conducted on the printer.
 - e. Test if all the configuration and parameterization saved on the printer are functional.
 - f. Conduct backup test of the print server.
- IV. Ad-hoc maintenance will be conducted on the network equipment hardware.
 - a. The network hardware configuration is backed up.
 - b. Network hardware is patched with latest firmware updates.
 - c. Physical cleaning (blowing) of the network hardware to remove all the dust.
 - d. Health inspection is then conducted on the network hardware.
 - e. Test if all the configuration and parameterization saved on the network hardware are functional.
 - f. Conduct backup test of the network hardware.
- V. Quarterly maintenance will be conducted on all the server room equipment
 - a. The air conditioners undergo service and cleaning on-site including functional testing.

- b. There is regular servicing of generators based on the engine runtime.
 - c. Regular checks on the access control are done to monitor functionality.
 - d. The fire systems undergo servicing and functional testing.
 - e. The CCTV systems are monitored, and issues detected. Upgrades are also done every 5 years.
- VI. Ad-hoc maintenance will be conducted on the air-conditioners and standby generators.
 - a. The network hardware configuration is backed up.
 - b. Network hardware is patched with latest firmware updates.
 - c. Physical cleaning (blowing) of the network hardware to remove all the dust.
 - d. Health inspection is then conducted on the network hardware.
 - e. Test if all the configuration and parameterization saved on the network hardware are functional.
 - f. Conduct backup test of the network hardware.

8.7 Monitoring

- I. For the Hyper-V server and storage environment, the Hyper-V and Failover Cluster Manager are utilised for the servers for monitoring.
- II. Sophos anti-virus detection also enabled on the servers for security breach alerts.
- III. There are screen records of administrator activities on desktops and laptops to monitor activity.
- IV. The UPSs and printers are monitored via web consoles to determine status and any error events.
- V. The storage devices are regularly monitored via the Netapp Management Console.
- VI. All network equipment hardware is monitored via the management consoles, where applicable.
- VII. All CCTV cameras are monitored via the CCTV system consoles.

8.8 Reporting

- I. All the ICT infrastructure and technology monitoring dashboards are monitored on a daily basis.
- II. The dashboards report on server resource usage, disk usage, and network.

- III. All server incidents are first investigated and resolved internally.
- IV. If an incident doesn't get resolved internally then a call is logged for escalation with the relevant service provider or Original Equipment Manufacturers (OEMs).
- V. Remote management tools are also utilised.
- VI. There is also AD Audit Plus to provide administrator activity logs and records.
- VII. Applications and systems do generate audit reports and logs.

9. GOVERNANCE ISSUES/AUTHORITY/DELEGATIONS

The policy will be administered by the ICT Manager's office and all the maintenance schedules should be communicated to the ICT Manager's office.

10. COMPETENCE AND CAPACITY TO IMPLEMENT THE POLICY

- 11.1 The Policy should be available and communicated to all staff
- 11.2 All staff should be aware of the prescriptions of the policy
- 11.3 All staff should be aware of the procedures contained in this policy
- 11.4 Supervisors/Managers should ensure compliance with this policy

11. CLASSIFICATION TABLE

Governance		
Sub classification	N/A	None
Title	ICT Infrastructure Management and Maintenance Policy	
File Number		
Related Policies or Procedures	• Information Security Policy • End User Information Security Policy	

	• Business Continuity Management Policy • Records Management Policy
<i>Responsible Officer</i>	• Mr B. Bakaco – Manager: ICT
<i>Original Authors</i>	• Mr B. Bakaco – Manager: ICT
<i>Current Author</i>	• Mr B. Bakaco – Manager: ICT
<i>Recommendation by ICT Manager (Date)</i>	
<i>Signature</i>	
<i>Support by SSD Director (Date)</i>	
<i>Signature</i>	
<i>Approval by Municipal Manager (Date)</i>	
<i>Signature</i>	
<i>Approved by Council Resolution (Date)</i>	
<i>Report No.:</i>	
<i>Effective date</i>	April 2024
<i>Next Review Date</i>	March 2025