



DR NKOSAZANA DLAMINI ZUMA MUNICIPALITY

Patch Management Policy

1. Introduction

Dr Nkosazana Dlamini Zuma Local Municipality is responsible for ensuring the confidentiality, integrity, and availability of data that is stored on its systems. Dr Nkosazana Dlamini Zuma Local Municipality has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

This policy has been developed considering the following prescripts and or acts:

- Promotion of Access to Information Act (Act no 43 of 1996);
- Electronic Communications and Transactions Act (Act no 25 of 2002);
- The Constitution of the Republic of South Africa (Act 108 of 1996)
- The protection of Information Act (Act 84 of 1982)
- The Municipal Finance Management Act (act 1 of 2002)
- Organizational policies and Procedures

2. Purpose

This document describes the requirements for maintaining up-to-date operating system security patches on all Dr Nkosazana Dlamini Zuma Local Municipality owned and managed workstations and servers.

3. Scope

This policy applies to workstations or servers owned or managed by Dr Nkosazana Dlamini Zuma Local Municipality. This includes systems that contain data owned or managed by Dr Nkosazana Dlamini Zuma Local Municipality regardless of location. The following systems have been categorized according to management:

- Servers (Running Windows Server Operating System) are managed by ICT Unit.
- Workstations (desktops and laptops) managed by ICT Unit

4. Policy

Workstations and servers owned by Dr Nkosazana Dlamini Zuma Local Municipality must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by Dr Nkosazana Dlamini Zuma Local Municipality.

5. Workstations

Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by Dr Nkosazana Dlamini Zuma Local Municipality.

6. Servers

Servers must comply with the minimum baseline requirements. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level

required to ensure the security of the Dr Nkosazana Dlamini Zuma Local Municipality systems and the data that resides on the system.

7. Roles and Responsibilities

- **The ICT Unit** will manage the patching needs for the Microsoft Windows servers and all workstations on the network.
- **The ICT Unit** is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
- **The Accounting Officer** is responsible for approving the patch management deployment requests.

8. Monitoring and Reporting

The ICT Unit is required to compile and maintain reporting that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

9. Enforcement

The ICT Unit is responsible for the implementation of this policy. The ICT Unit may conduct random assessments to ensure compliance with policy without notice. Any system that is not updated according to the direction of this policy shall require immediate corrective action.

10. Definitions

Term	Definition
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
	Trojan A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

11. Conclusion

This policy should allow a manageable level of preparedness and add a critical extra layer to ICT Security, provided it works hand in hand with ICT Disaster Recovery and Backup Policy.

Signature	Approved by	Date
	Sj Sondezi	28 May 2026