

ELIAS MOTSOLEDI LOCAL MUNICIPALITY



PATCH MANAGEMENT POLICY

MUNICIPAL COUNCIL RESOLUTION NUMBER

M24/25-07

APPROVED AT THE COUNCIL MEETING OF DATE 10 AUGUST 2024

MR

M.D

Table of Contents

Overview	3
Purpose	3
Scope	3
Update Requirement Determination	3
Types of patches	3
Patching Priorities	4
Patch Priority Matrix	4-5
Enforcement	5

1. Overview

The goal of the patch management policy is to guarantee that computer software is promptly updated or patched to lessen or eliminate the chance of unauthorised access to the municipality's workstations and servers.

This is an internal IT policy that outlines the circumstances and frequency of computer system updates

2. Purpose

The purpose of the policy is to establish a minimum process for protecting the organizational computers on the network from security vulnerabilities. It shall determine how updates are done for both servers and workstations and who is responsible for performing the updates along with specifying the tools used to perform system updates.

3. Scope

This policy applies to all ICT-related purchased software, servers, printers, and computers owned and operated by Elias Motsoaledi Local Municipality.

4. Update Requirement Determination

This section defines methods used to determine what updates should be done and when they should be applied.

Update Checking

Several methods would be used to determine when updates should be performed.

1. Notifications of patches from application and application vendors will be reviewed and the patches will be implemented appropriately. Where notifications are not automatically sent, the supplier's website will be reviewed regularly.
2. The websites of the suppliers of servers, PCs, switches, routers, and peripherals will be reviewed to determine the availability of firmware patches.
3. Missing patches identified will be implemented as appropriate. Any weaknesses identified will be rectified.
4. Any system updates/patches for Linux operating systems will be done by the relevant service provider, tested, and implemented.

5. Types of patches

The following patches or updates will be implemented on different infrastructure types.

Infrastructure Type	Patch type
Server/ Computer/printers	Drivers / Firmware
operating System	Service packs

Mr

M.D

Application Software	Service packs
Routers / Switches	Firmware
Anti-virus / Antispyware	Anti-virus updates

6. Patching Priorities

The following Patch Priority Matrix represents all systems and applications at Elias Motsoaledi Local Municipality, their relative priority for patching, and timeframes within which the patches must be applied (e.g. immediately, regularly, monthly, or quarterly).

The following indicates how Elias Motsoaledi Local Municipality categorizes patches:

6.1 Critical Priority Patches

Critical patches are security-oriented and address vulnerability exploits known to have occurred. The patches resolve vulnerabilities that can be accessed remotely via the Internet or a network. Three days after the vendor releases these updates, they will be implemented.

6.2 High Priority Patches

Are those patches that are security-oriented, all the conditions that make a patch Critical also make it high EXCEPT that there is no evidence of exploits existing for the vulnerability. Where possible patches will be tested and applied within one week of release

6.3 Moderate Priority Patches

Moderate patches are also security-oriented patches; however, these patches only address vulnerabilities that can be exploited locally, meaning, an attacker needs to have local access to the machine.

6.4 Low-Priority Patches

Are patches of a Low priority encompassing all other types of patches, the patch is NOT security-oriented (it might add new functions to a program, for example), it does not address any kind of vulnerability, and it does not have any severity rating.

7. Patch Priority Matrix

System/Application	Application Criticality	High Priority Patch	Moderate Priority Patch	Low Priority Patch
[Anti-virus]	[High]	[Immediate]	[Immediate]	[Immediate]
[Servers]	[High]	[Immediate]	[weekly]	[Weekly]

MR

M.D

[Operating System Updates]	[Medium]	[Immediate]	[Weekly]	[Weekly]
[Firewall]	[High]	[Immediate]	[Immediate]	[Immediate]
[VIP payroll]	[Medium]	[Monthly]	[Monthly]	[Monthly]

7.1. Vulnerability assessment and system patching will only be performed by System Administrators & Network Administrators.

7.2. Vulnerability scanning of systems will take place daily systematically to stay up to date.

7.2.1 Kaspersky Endpoint Security is used for scanning vulnerabilities/ software updates for servers, desktops, and laptops to improve the speed and proper functionality of the system.

7.2.2 VIP payroll system updates shall be performed by the System Administrator while all application users are completely shut down/logged out to allow the updates to be successful.

7.3. Before implementation, every vulnerability warning and patch release will be compared to the current EMLM systems and services because not all patches address problems or real system versions the municipality is exhausting.

7.4. The decision to apply a patch, and within what timeframe, must be made following the guidelines presented in the Patch Priority Matrix.


7.5. Patches will be implemented with the least interference to Municipality operations possible.

7.4. Audits will be performed monthly to ensure that patches have been applied as required and are functioning as expected.

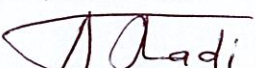
8. Enforcement

Employees who purposely violate this policy may be subject to Elias Motsoaledi Local Municipality disciplinary procedures including denial of access. Any employee aware of any violation of this policy is expected to report to their supervisor or other authorised representative.

9. Signatories


 Ms. NR Makgata RrTech Eng
 Municipal Manager

30/08/2024
 Date


 The Mayor
 Cllr. Tladi DM

30/08/2024
 Date