

DR NDZ LOCAL MUNICIPALITY



ICT PATCH MANAGEMENT POLICY

Core Business Areas	Corporate Services Department
Operational Area	IT Unit

Version	
Date	
File Name	PATCH MANAGEMENT POLICY
Business Owner	Corporate Services Manager
Date Approved	

Document Classification:
Confidential
©Ingwe Local Municipality 2015

PATCH MANAGEMENT POLICY

Index

- 1. Purpose**
- 2. Varying Levels of Patches**
- 3. Patch Management**
- 4. Patch Procedure**
- 5. Reporting**
- 6. Conclusion**

This is a formal Patch Management Policy for Ingwe local Municipality.

1. Purpose

Given that the Municipality has numerous complex interconnected systems with an internet connection, it is to be expected that vulnerabilities may be discovered on these systems on a

regular basis. Such vulnerabilities are comprehensively managed by the providers of the hardware and software involved, and so (as long as ICT Security is adhered to) the only immediate concerns are ensuring A) That patches are applied as quickly as possible and B) That patches do not break existing functionality.

2. Varying Levels of Patches

Patches address varying levels of security issues, and some exist purely to add additional functionality to the system involved. While there tends to be varying nomenclature between providers, patch types can largely be broken down into Critical, Important, Moderate and Low. Critical patches should be regarded as mitigation of a threat already in existence 'in the wild', and therefore as an urgent requirement to prevent loss or unauthorised access of data.

3. Patch Management

At the municipality, there are multiple programs considered critical for business that all require patching on a fortnightly basis or less. Among these are:

- i. Adobe Reader
- ii. Eset Antivirus
- iii. Microsoft Windows
- iv. Microsoft Office
- v. Hardware specific driver updates
- vi. Java
- vii. Linux server
- viii. Windows Server

Some of these programs (Eset, Microsoft) support the use of a central server to manage update downloads, which can assist with tracking updates and patch levels of various systems. Other updates must be tracked on a 'per pc' basis.

4. Patch Procedure

This can be broken down by supplier:

- i. Adobe Reader: Must be manually monitored on workstations on a biweekly basis
- ii. Eset Antivirus: Central antivirus server to be established in the office, and clients configured to use this server.
- iii, iv and v. Microsoft Windows, Office and Hardware Specific Driver Updates: The Windows Server is to be set up so that updates can be downloaded and monitored from this server.
- vi. Java: To be monitored on a biweekly basis for affected workstations. Worth noting is that workstations making use of Easy file require an older version of Java, and cannot be updated.
- vii. Linux Server: The Linux server is updated weekly or immediately in the case of a critical patch or vulnerability, with reports available on actions taken.

Viii. Windows Server: The Windows server is to be configured to automatically download and install updates for itself.

5. Reporting

Patches are to be monitored, and so a report is to be generated monthly of patches applied, and is to be signed off by the ICT Manager. This sign-off must detail the vendor, affected workstations and relevant date.

6. Conclusion

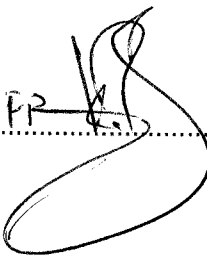
This policy should allow a manageable level of preparedness and add a critical extra layer to ICT security, provided it works hand in hand with the ICT Disaster Recover and Backup Policy.

COUNCIL APPROVAL AND EFFECTIVE DATE

Approval of Policy by Council and Effective date: 06/06/2017

MUNICIPAL MANAGER

DATE


.....

19/06/2017
.....