PATCH MANAGEMENT POLICY AND PROCEDURES

MUNISIPALITEIT
RICHTERSVELD
MUNICIPALITY

Approved Date: 29 August 2017	**Council Resolution Nr: RVN 020/08/2017**
Effective Date: 01 September 2017	**Review Date: 30 Junie 2018**

OVERVIEW

The goal of patch Management is to keep the components that form part of information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

Vulnerability and patch management is an important part of keeping the components of the information technology infrastructure available to the end user. Without regular vulnerability testing and patching, the information technology infrastructure could fall foul of problems which are fixed by regularly updating the software, firmware and drivers. Poor patching can allow viruses and spyware to infect the network and allow security weaknesses to be exploited.

1. PURPOSE

1.1 This policy defines the procedures to be adopted for technical vulnerability and patch management.

2. SCOPE

2.1 This policy applies to all components of the municipality's information technology infrastructure and includes as well as all crucial system of the municipality:-

- Computers
- Servers
- Application Software
- Peripherals
- Routers and switches
- Databases
- Storage

All staff within the ICT Department must understand and use this policy. ICT staff are responsible for ensuring that the vulnerabilities within the IT infrastructure are minimised and that the infrastructure is kept patched up to date.

All users have a role to play and a contribution to make by ensuring that they allow patches to be deployed to their equipment.

3. RISKS

Without effective vulnerability and patch management there is the risk of the unavailability of systems. This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.

4. POLICY

The municipality's ICT infrastructure will be patched according to this policy to minimise vulnerabilities.

IDENTIFYING PATCHES TO BE APPLIED

- The organisation's anti-virus server will be configured to automatically down load the latest virus and spyware definitions.
- Windows patch management tools will be utilised to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.
- Notifications of patches from application and database vendors will be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the suppliers website will be reviewed on a regular basis.
- The websites of the suppliers of servers, PC's, tablets, printers, switches, routers and peripherals will be reviewed to determine the availability of firmware patches.
- Missing patches identified will be implemented as appropriate. Any weaknesses identified will be rectified.
- Any system updates/patches for Linux operating systems must be done by the relevant service provider, tested and implemented.
- For all updates on Linux operating systems, the Change control process must be followed, to ensure successful completion of update and minimize any problems that might occur.

TYPES OF PATCHES

The following patches will be implemented on the different information infrastructure types.

TYPE	PATCH
Server/ Computer	Drivers/ firmware
Operating system	Service packs
Application software	Service packs, feature packs
Routers and Switches	Firmware
Printers	Drivers, firmware
Scanners	Drivers, firmware
Anti-virus/ Anti spyware	Data file/ Virus definition update.

ROLES AND RESPONSIBILITIES

The ICT Department will be responsible for identifying patches for the application systems which they administer.

ICT Department will also be responsible for patch approval and ownership of all technical updates including: operating systems, patches for workstations and servers, antivirus and antispyware, drivers of devices

The ICT Department will use restore points where practical to ensure rollback changes.

PATCHING SCHEDULE

The municipality's ICT Department infrastructure will be patched according to this schedule.

Workstations should be patched according to the schedule below

TIME	ACTION
Weekly	Antivirus and spyware definitions configured to be installed as they are released.
Quarterly	Microsoft critical updates and security updates configured to be approved for rollout as they are released.
Quarterly	Check that drivers are up to date.

Windows Servers should be patched according to the schedule below.

TIME	ACTION
Weekly	Antivirus and spyware definitions will be configured and installed as they are released. Critical Security patches installed.
Monthly	All outstanding patches.
Quarterly	Check that drivers are up to date.

Printers, peripherals, switches and routers and storage should be patched according to the schedule below.

TIME	ACTION
Annually	Check for new firmware updates

POLICY REVIEWS

At present there is a Clause in all approved policies whereby it be reviewed annually by the Council.
There is however only a certain number of policy statements (e.g. finance related) that must be reviewed annually according to legislation.

AUTHORITY

MM Approval: Date:

Council Approval: Date: