KGATELOPELE LOCAL MUNICIPALITY

PATCH MANAGEMENT POLICY AND PROCEDURES

2016/2017

Overview
The goal of vulnerability and 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 information technology infrastructure and includes:-
• Computers
• Servers
• Application Software
• Peripherals
• Routers and switches
• Databases
• Storage

2.2 The IT Intern must understand and use this policy. IT staff are responsible for ensuring that the vulnerabilities within the IT infrastructure are minimised and that the infrastructure is kept patched up to date.
2.3 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
3.1 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 This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.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

4.1 The organisation's IT infrastructure will be patched according to this policy to minimise vulnerabilities.

4.2. Identifying Patches to be applied

4.2.1 The organisation's anti-virus server will be configured to automatically down load the latest virus and spyware definitions.

4.2.2 Windows patch management tools will be utilised to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.

4.2.3 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.

4.2.4 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.

4.2.5 Missing patches identified will be implemented as appropriate. Any weaknesses identified will be rectified.

4.3 Types of Patches

4.3.1 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 / Scanners	Drivers, firmware
Anti virus/ Anti spyware	Data file/ Virus definition update.

4.4 Roles and Responsibilities

4.4.1 The IT Intern will be responsible for identifying patches for the application systems which they administer.

4.4.2 IT Intern 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.

4.4.3 IT Department will use restore points where practical to ensure rollback changes.

4.5 Patching Schedule

The organisation's IT 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.
Monthly	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

Approved: Date:

…… ……

Municipal Manager