Pixley ka Seme District Municipality

PATCH MANAGEMENT POLICY AND PROCEDURE

Overview

The Patch Management Policy is intended to ensure that computer software is patched or updated in a timely manner to reduce or prevent the possibility of unwanted intrusion on servers and workstations of the municipality.

This is an internal IT policy which defines how often computer system updates are done and under what conditions they are done.

Purpose

This policy is required 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.

Scope

The Patch Management Policy applies to all computer equipment operated by the District Municipality or functioning on the organizational network. All third parties operating computer equipment on the organizational network must have an acceptable patch management solution which is kept current and active. This policy is effective as of the issue date and does not expire unless superseded by another policy.

Update Requirement Determination

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

Update Checking

There are several methods that 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 applied as appropriate. Where notifications are not automatically sent, the supplier's website will be reviewed on a regular basis.
2. The websites of the suppliers of servers, PC's, 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.

The review of posted security flaws and patches should always be used for the computer operating system, BIOS, and applications. The manufacturer website should be used and there may also be other appropriate sites posting relevant bulletins. If automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.

MTK

Types of patches

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

Infrastructure Type	Patch type
Server / Computer	Drivers / Firmware
Operating System	Service packs
Application Software	Service packs
Routers / Switches	Firmware
Anti-virus / Antispyware	Anti-virus updates

User Responsibilities

All users must be informed about the importance of having updates to their computers and the possible consequences of failure.

- Users must not disable the ability of their workstation to be updated.
- Users must immediately notify the IT Support Officer if they suspect that their workstation is not receiving updates.
- The IT Support Officer will use restore points where practical to ensure changes are rolled back; this would be done to undo changes made by faulty updates or patches.

Enforcement

Since patch management is important to maintain the security of the organizational network and prevent unauthorized data disclosure, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

EXECUTIVE MAYOR : _____

DATE APPROVED : **30 AUGUST 2017**

RESOLUTION : **R 2017 – 08 – 30 (9.3)**