KAMIESBERG
MUNISIPALITY
"gems galore from mountains to shore"
REAL GEMS
REAL EXPERIENCES
REAL ART

KAMIESBERG MUNICIPALITY PATCH MANAGEMENT POLICY

2. TABLE OF CONTENTS

3. 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. This policy is to be implemented immediately and will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the Municipality's needs and goals Vulnerability and patch management is an important part of keeping the components of the information technology infrastructure available to the end user.

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.***

4. Purpose

This policy defines the procedures to be adopted for technical vulnerability and Patch Management.

5. Scope

This policy applies to all components of the information technology infrastructure and includes:-

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

All staff within the IT Department 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. All users of users have a role to play and a contribution to make by ensuring that they allow patches to be deployed to their equipment.

6. Enforcement

If any staff member/employee of the Municipality is found to have breached this policy, they may be subject to disciplinary action. Users who systematically breach this policy by failing to allow the equipment that they use to be updated, may be subject to disciplinary action.

7. 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 This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.

8. Patch Management Policy

The following guidelines and procedures apply to this policy.

- The Municipality's IT infrastructure will be patched according to this policy to minimise vulnerabilities.
- System components and other I.T. resources need to be patched on a secure and consistent basis to avoid unwanted damage to all environments.
- The IT department will be responsible for keeping the database accurate and relevant.
- Patch Management has become a critical security issue, therefore all system components directly associated with the Municipality's data environment must be securely hardened and configured with all necessary and appropriate patches and system updates for preventing the exploitation or disruption of mission-critical services.
- In accordance with best practices for Security Patch Management, the subsequent three (3) security concerns will be highlighted throughout the Security Patch Management policy. They are as follows:

Vulnerabilities: Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the Municipality's data environment or any other I.T. resources

Remediation: The three (3) primary methods of remediation are:
Installation of a software patch

Adjustment of a configuration setting

Removal of infected software.

Threats: Threats are capabilities or methods of attack developed by malicious entities to exploit

Vulnerabilities and potentially cause harm to a computer system or network. Common examples are ***scripts***, ***worms***, ***viruses*** and ***Trojan horses***.

- Failure to keep system components and other I.T. resources patched on a secure and consistent basis can cause unwanted damage to all environments. This includes, but is not limited to the following:
  - Network devices and all supporting hardware and protocols
  - Operating systems within the development and production environments
  - Applications within the development and production environments
  - Databases within the development and production environments
  - Any other mission-critical resources within the data environment that require patches and security updates for daily operations

- A comprehensive SPMP (Security Patch Management Program) which encompasses the categories and supporting activities listed below, need to be developed and implemented:
  - A formalized Security Patch Management Program employee, complete with his/her roles and responsibilities
  - Comprehensive inventory of all I.T. resources.
  - Procedures for establishing priorities regarding Security Patch Management. This will include, but is not limited to

(1) the significance of the threat,
(2) the existence and overall threat of the exploitation
(3) the risks involved in applying Security Patch Management procedures (its affect on other systems, resources available and resource constraints).

- The creation of a database of remediation activities that needs to be applied
- Test procedures for testing patches regarding remediation
- Procedures for the deployment, distribution and implementation of patches and other related security-hardening procedures
- Procedures for verifying successful implementation of patches and other related security-hardening procedures

These policy directives will be fully enforced by the Municipality to ensure the SPMP initiatives are executed in a formal manner and on a consistent basis for protecting all system components and I.T. resources in all applicable environments. Various external security sources and resources are utilized to ensure that the Municipality maintains awareness of security threats, vulnerabilities and what respective patches, security upgrades and protocols are available.

It is the responsibility of the IT department to verify the successful implementation of all patches and security upgrades to the Municipality's I.T. infrastructure. These activities will consist of, but are not limited to the following:

- Verifying that the files have been changed as stated in the vendor's documentation to reflect the updates as needed
- Verifying whether the recommended patches and security updates were installed properly by reviewing patch logs

9. Responsibility for Policy Maintenance

It is the responsibility of the IT department to ensure that the aforementioned policy is kept current and updated. The IT department must also perform audits to ensure that the policy is adhered to and enforced correctly.