**UMTSHEZI MUNICIPALITY**



**PATCH MANAGEMENT POLICY**

**Patch Management Policy**

**Approval and Version Control**

|  |  |  |
| --- | --- | --- |
| **Approval Process:** | **Position or Meeting Number:** | **Date:** |
| Originator |  |  |
| Recommended by Director of Corporate Services |  |  |
| Recommended by EXCO |  |  |
| Approved by Council | Res 270.06.14 | 14/06/2014 |
| Effective |  |  |
| Review Frequency: Once a year (i.e. Annually) | Res 120.07.15 | 14/07/2015 |
| Version Number |  |  |

**TABLE OF CONTENTS**

[1. OVERVIEW 4](#_Toc373393557)

[2. PURPOSE 4](#_Toc373393558)

[3. SCOPE 4](#_Toc373393559)

[4. DEFINITIONS 4](#_Toc373393560)

[5. GENERAL POLICY 5](#_Toc373393561)

[6. PATCH MANAGEMENT 5](#_Toc373393562)

[6.1. IT OFFICER RESPONSIBILITIES 5](#_Toc373393563)

[6.2. SERVICE PROVIDER RESPONSIBILITIES 6](#_Toc373393564)

[6.3. ALL STAFF & THIRD PARTIES 6](#_Toc373393565)

[6.4. THE MUNICIPALITY 6](#_Toc373393566)

[6.5. MONITORING 6](#_Toc373393567)

[6.6. ASSESSING AND CLASSIFYING RISK 7](#_Toc373393568)

[6.7. TESTING 7](#_Toc373393569)

[6.8. AUTHORISATION AND NOTIFICATION 8](#_Toc373393570)

[6.9. IMPLEMENTATION 8](#_Toc373393571)

[6.10. VERIFICATION 9](#_Toc373393572)

[7. HOT FIXES 10](#_Toc373393573)

[8. ENFORCEMENT 10](#_Toc373393574)

[9. APPENDICES 10](#_Toc373393575)

[9.1. Appendix A - Patch Control Form 10](#_Toc373393576)

[9.2. Appendix B - Monthly Patch Management Compliance Form 10](#_Toc373393577)

# OVERVIEW

This Policy establishes certain requirements which must be met by all computers and servers connected to the Umtshezi Municipality network to provide the municipality with a trusted and secure network infrastructure to support the effective delivery of IT resources and mechanisms to help the organisation realise its goals and objectives in maintaining a secure IT environment. It attempts to set standards in terms of patch management.

# PURPOSE

It is the IT Officer's responsibility to ensure that all computer devices (including servers and desktops) that are connected to the Umtshezi Municipality network have the latest security patches installed. This document describes the management of IT Security/Integrity Patches for the Umtshezi Municipality. This document provides a common definition of what is required when performing Security Patch Management activities for the Umtshezi Municipality.

# SCOPE

The scope for this process comprises the following:

* IT Security/Integrity Patches, which includes Security Updates and Hot Fixes.
* Systems/Platforms, Hardware and Applications.
* All software on all platforms and devices.

# DEFINITIONS

**Patches** - typically released to protect against known exploits in operating system or application code or to address functionality issues or a new vulnerability.

**Vulnerabilities** - weaknesses in software that can be exploited by an entity to gain elevated privileges is authorised to have on a computer or system. Not all vulnerabilities have related patches. These situations require workarounds to attempt to mitigate “un-patched” vulnerabilities.

**Threats** - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

**CERT** - CERT is the Internet's official emergency team. CERT focuses on security breach and incidents, providing alerts and incident-handling and avoidance guidelines. CERT also conducts an on-going public awareness campaign and engages in research aimed at improving security systems.

# GENERAL POLICY

* 1. Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, approval, installing and verifying.
  2. Umtshezi Municipality is committed to complying with applicable compliance laws, rules and standards.

# PATCH MANAGEMENT

## IT OFFICER RESPONSIBILITIES

* + 1. The IT Officer must ensure that all IT systems are patched in timely manner as detailed in this policy.
    2. The IT Officer must review current threats and vulnerabilities and check relevant advisories to monitor for patches or fixes to mitigate the risks presented by these threats and vulnerabilities.
    3. The IT Officer must establish and implement a departmental program for patch management on all IT systems.
    4. The IT Officer must ensure that a departmental inventory of hardware and software patch status is developed to maintain and track the status of all patch actions and vulnerability corrections and to provide rapid response to internal or external reporting requirements.
    5. A Patch Management Compliance form (see Appendix B) must be completed by the IT Officer for all patches installed. The IT Officer will take overall responsibility in ensuring that patches are applied.
    6. The IT Officer must report the patch management status of the municipality on a monthly basis to the Director of Corporate Services using the Patch Management Compliance Form.
    7. The IT Officer must develop and publish policy and procedural guidance on patch management.
    8. The IT Officer must monitor patch management on a municipal-wide basis.

## SERVICE PROVIDER RESPONSIBILITIES

* + 1. The relevant service provider must ensure that security patches/ hot fixes for Venus and Microsoft products are performed in a timely manner as laid out in this policy.
    2. The relevant service provider must review current threats and vulnerabilities and to check relevant advisories to monitor any potential threats or vulnerabilities.
    3. The relevant service provider must report the patch management status of the municipality on a regular basis to the IT Officer.

## ALL STAFF & THIRD PARTIES

* + 1. It is the responsibility of each user, both individually and within the municipality, to ensure prudent and responsible use of computing and network resources.
    2. End Users must report any suspected lack of compliance with this policy to the IT Officer. Failure to do so constitutes a violation of this policy.

## THE MUNICIPALITY

* + 1. Reserves the right to monitor for violations of this policy.

## MONITORING

* + 1. The IT Officer and relevant service provider will monitor and/or subscribe to security mailing lists, review vendor notifications and web sites and research specific public web sites for the release of new patches.
    2. Monitoring will include, but not be limited to, the following:
       1. Scanning the Umtshezi Municipality’s’ network to identify known vulnerabilities.
       2. Monitoring Computer Emergency Readiness Team, CERT, other advisories and websites of all vendors that have hardware or software operating on the municipality’s network.
       3. Where a vendor has no subscription service available for the notification of patches that are released, the IT Officer and relevant service provider will perform manual monitoring at least monthly.

## ASSESSING AND CLASSIFYING RISK

* + 1. Once alerted to a new patch, the IT Officer or relevant service provider will download and review the new patch.
    2. The security patch will be assessed for risk and severity and a classification will be assigned.
    3. The patch will be categorized based on the criticality of the patch according to the following:
       1. Emergency - an imminent threat to the Umtshezi Municipality’s’ network.
       2. High – A vulnerability whose exploitation could allow the propagation of malicious software without user action. A vulnerability whose exploitation could result in compromise of the confidentiality, integrity or availability of user’s data or of the integrity or availability of processing resources.
       3. Medium - Exploitability is mitigated to a significant degree by factors such as default configuration, auditing or difficulty of exploitation.
       4. Low – A vulnerability whose exploitation is extremely difficult or whose impact is minimal.

## TESTING

* + 1. The IT Officer or relevant service provider will assess the effect of a patch to the municipality’s’ infrastructure prior to its deployment.
    2. The IT Officer will assess the affected patch for criticality relevant to each platform (e.g., servers and desktops).
    3. All patches will undergo testing for each affected platform before release for implementation.
    4. If a patch is categorised as an Emergency, it is considered an imminent threat to Umtshezi Municipality’s’ network. Therefore, the Umtshezi Municipality assumes greater risk by not implementing the patch than waiting to test it before implementing.
    5. Once the IT Officer or relevant service provider is satisfied that the implementation of a new patch will not cause any unexpected behaviour, he must agree upon a schedule for implementation.
    6. It is the responsibility of application end users to identify any problem(s) with a patch or patches and to notify the IT Officer of the problem(s) post installation.

## AUTHORISATION AND NOTIFICATION

1. Regardless of criticality, each patch requires the creation and approval of a request for change prior to implementing the patch.
2. Patches classified as ‘Emergency’ will follow the Emergency Change control procedures. .
3. The IT Officer or relevant service provider will implement patches during regularly scheduled maintenance (downtime) periods.
4. The Director of Corporate Services must approve the patch schedule prior to implementation.
5. For new network devices and servers, each platform will follow established hardening procedures to ensure the installation of the most recent patches.
6. Since a security patch may cause a system to malfunction, the IT Officer should proactively announce the implementation of a patch or patches.

## IMPLEMENTATION

* + 1. The IT Officer or relevant service provider will implement Emergency patches within eight hours of availability. As Emergency patches pose an imminent threat to the network, the implementation may precede testing.
    2. In all instances, the IT Officer or relevant service provider will perform testing pre-implementation and document it for auditing and tracking purposes.
    3. The IT Officer will obtain authorisation for implementing Emergency patches via an emergency change (refer to the IT Change Management Procedure).
    4. The IT Officer or relevant service provider will implement High, Medium and Low patches during regularly scheduled maintenance (downtime) windows. Each patch will have an approved change record.
    5. Patches will be implemented on all devices according to the timeframes below:

|  |  |
| --- | --- |
| **Criticality of Patch** | **Timeframe to Implement** |
| Emergency | Within 8 hours of availability |
| High | Within 30 days of availability |
| Medium | Within 60 days of availability |
| Low | Within 90 days of availability |

## VERIFICATION

* + 1. Following the implementation of all patches, the IT Officer or relevant service provider will verify the successful installation of the patch to ensure that there have been no adverse effects.

# HOT FIXES

* 1. Operating system updates, hotfixes and service packs will only be installed under the following conditions:
     1. If a specific issue has been identified that requires the installation of the update, hotfix or service pack.
     2. All relevant documentation for the update, hotfix or service pack has been reviewed to determine any configuration changes and potential problems that may be introduced and to determine whether all requirements for installation are being met.
     3. The update, hotfix or service pack has been installed and tested in a test environment to determine any possible issues that may result in the production environment.
     4. It has been established that there is a greater risk in not applying the update, hotfix or service pack then there is in the risk of applying it.

# ENFORCEMENT

* 1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# APPENDICES

### Appendix A - Patch Control Form

### Appendix B - Monthly Patch Management Compliance Form

**APPENDIX A - PATCH CONTROL FORM**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PATCH INFORMATION:** | | | | | | | | | | |
| Patch Source or Vendor Name (if Patch was alerted to municipality by system vendor): | |  | | | Email: | | |  | | |
| Date Requested: | |  | | | Contact No.: | | |  | | |
| Signature: | |  | | | Office: | | |  | | |
| System Affected: | |  | | | Patch Request No: | | |  | | |
| **DESCRIPTION OF PATCH** | |  | | | Risk Rating: | | |  | | |
| **BUSINESS JUSTIFICATION** | |  | | | | | | | | |
| **NATURE AND PRIORITY** | |  | | | | | | | | |
| **AUTHORISATION AND APPROVAL** | | | | | | | | | | |
|  | | **Name** | **Title** | | | **Date** | | | **Signature** | |
| **Approved by:** | |  |  | | |  | | |  | |
| **Authorised by:** | |  |  | | |  | | |  | |
| **TESTING OF CHANGES** | | Testing Required : YES / NO  If “NO”, provide reason for not testing:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Testing Documentation/Screen Prints – Attached to Change Request: YES / NO | | | | | | | | |
| **SIGN-OFF COMPLETION OF CHANGE** | | | | | | | | | | |
|  | **Name** | | | **Title** | | | **Date** | | | **Signature** |
| **Tested by (where applicable):** |  | | |  | | |  | | |  |
| **Patch Implemented by:** |  | | |  | | |  | | |  |

**APPENDIX B - PATCH MANAGEMENT COMPLIANCE FORM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Patch Request Number:** | **Details of Change:** | **Change Documentation Attached:** | **Change Management Process Followed: (Yes/No)** | **Details of Exceptions Noted:** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **Checked by:** |  | | | |
| **Designation:** |  | | | |
| **Sign:** |  | | | |
| **Date:** |  | | | |