APPLICATION PATCH MANAGEMENT POLICY

APPROVED BY:

MR M NAKO

MUNICIPAL MANAGER

DATE: 21/06/2023

APPROVED BY:

CLLR S JANDA

EXECUTIVE MAYOR

DATE: 21/06/2023

1. POLICY BACKGROUND

The dependency on information technology (IT) has increased progressively for organizations as a strategically important competitive advantage. According to the King IV, It's about the ability of the enterprise's board to **evaluate**, **direct** and **monitor** the use of an enterprise's technology and information resources in support of the achievement of the *organisation's strategic objectives*.

Patch management has become a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. Consequently, all the municipality's applications must be securely hardened and configured with all necessary and appropriate patches and system updates to prevent the exploitation or disruption of mission-critical services.

2. POLICY PURPOSE

To manage patches or upgrades for software applications and technology to assist the municipality in handling changes effectively as per specific needs of each application at a given time to reduce vulnerability identified.

3. DEFINITIONS

Patch	Is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.
Patch Management	Is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.
Application/System	A system that provides a specific set of functions and/or services to end users in support of business objectives. The term is commonly associated with a specific software application such as a financial system.
Information System	Same as application above.

4. APPLICATION AND SCOPE

The scope of this policy and procedures covers the application of security patches for IT Applications within Mbhashe Local Municipality.

5. LEGISLATIVE FRAMEWORK

5.1 Constitution Act 108 of 1996
5.2 King IV Corporative Governance

6. POLICY PROCEDURE

This policy is applicable to ICT infrastructure and employees, including service providers offered systems to the municipality

7. GENERAL POLICY PROVISIONS

7.1 Statement of policy

7.1.1 The ICT Manager has a responsibility to ensure that the municipality's applications are safe, secure, and are operational at all times.

7.1.2 The application of patches and updates to these IT Applications plays a big role in ensuring that the availability, security and proper functioning of such IT Applications are maintained properly.

7.1.3 The System Administrator / ICT Administrator has the responsibility to coordinate or carry out all the activities related the application of patches to the municipality's IT Applications.

7.1.4 The following are the patch management tasks that the Applications Administrator must perform:

7.1.4.1.1 **Assessment** - determine what your current patching level is, identifying which patches are installed and which are missing.

7.1.4.1.2 **Monitoring** - watch out for alerts and new patch releases by the applications' vendors and trusted third parties.

7.1.4.1.3 **Review and Evaluation** - determine whether or not a particular patch applies to any of the municipality's applications, review its associated documentation, and determine its level of priority or criticality.

7.1.4.1.4 **Risk Assessment and Testing** - assess the effect of the patch by applying it on the test copy of the IT Application concerned prior to deploying to its production environment.

7.1.4.1.5 **Authorisation and Scheduling** - regardless of criticality, each patch release requires the creation and approval of a request for technical change prior to releasing the patch. The Director: Corporate Services is the official responsible for approving the schedule of patches prior to their implementation.

7.1.4.1.6 Deployment - when a patch has been successfully certified as ready for deployment and the necessary approval obtained, the System Administrator / IT Administrator should deploy the patch as per the procedures outlined in the Procedures section of this document.

7.1.4.1.7 **Post-deployment Review** - this review should be conducted afterwards to identify issues such as installation problems, process weaknesses and lessons learned. The aim to constantly improve our patch management processes.

8. PROCEDURES FOR IMPLEMENTING POLICY

8.1 Patch management procedures

The following are the patch management procedures that must be followed in patching the municipality's IT Applications:

8.2 ASSESSMENT

- If not already done, create a list of all IT Applications that are under the purview of the IT Section.
- Identify all the IT Applications that are critical to the business and sustainability of the municipality. These should always take priority in the municipality's patch management program.
- Determine what the current patching level is of each of the IT Applications in the list, identifying which patches are installed and which are missing.
- Systems that cannot be patched or raised to the same level as the rest of the municipality's applications should be identified, documented and be brought to the attention of senior management.

8.3 MONITORING

- Monitor the affected Applications' vendor websites and notifications on security vulnerabilities, known bugs and available patches to fix such.
- Research specific and trusted public websites and user groups for the release of new patches.
- Subscribe to vendor mailing lists in order to get alerts and patch release notifications on time.

8.4 REVIEW AND EVALUATION

- Once alerted to a new patch release, download and review the new patch within one day of receiving the notification.
- Review all of its associated documentation, including information such as prerequisites, known issues, functionality changes, alternative workarounds, and removal instructions.
- Assign a criticality (or priority) to each patch, so you can determine how quickly a patch must be deployed or what particular application would need a faster deployment.
- Categorise the criticality of the patch according to the following:
    - **Emergency** - an imminent threat to the municipality's IT Applications
    - **Critical** - targets a security vulnerability
    - **Important** - a standard patch release update containing updated functionality that is useful to the municipality.
    - **Low** - a standard patch release update that is released to deal with a very low security threat and/or may contain updated functionality that is not necessary for the municipality.

- **Not applicable** to the municipality's IT Applications
- The following are some of the questions necessary to determine the priority of a patch:
  - Are critical business applications impacted?
  - Are there mitigations in place that reduce the threat?
  - Is the vulnerability that the patch addresses being exploited out there?
  - Would a large number of applications/users be affected in case of an attack that exploits that vulnerability?
  - What information would be at risk if the application was left unpatched?

- Below is a table that represents the different priority levels/criticality and the recommended deployment timeframes:

Priority	Recommended Deployment Time Frame	Maximum Deployment Time Frame
1 – Emergency	Within 6 to 12 hours	Within 12 to 24 hours
2 – Critical	Within 1 to 2 days	Within 1 week
3 – Important	Within 2 weeks	Within 1 month
4 – Low	Within 3 months	Within 6 month
5 - Not Applicable	Not necessary	Not necessary

- The baseline for the timeframes stipulated above is the time the patch is successfully downloaded.

8.5 RISK ASSESSMENT AND TESTING

- Determine the impact of deploying the patch within the stated timeframe has on the business of the municipality and whether there is a workaround that might be preferable in the short term. The patch must still be scheduled for deployment at a later stage.
- Assess the effect of the patch by applying it on the test copy of the IT Application concerned prior to deploying to its production environment.
- Expedite the testing process for patches categorised as Emergency and Critical.
- Roll-back procedures should also be tested should roll-back be necessary.
- The results should be reviewed by at least two individuals, as it mitigates the risk that critical information might be missed.

8.6 AUTHORISATION AND SCHEDULING

- Regardless of criticality and upon passing the risk assessment and testing, each patch release requires the creation and approval of a request for technical change.

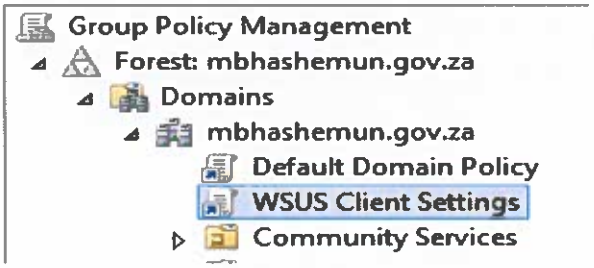
- The request and the schedule for the deployment of the patch should be submitted to the ICT Manager for the review and acceptance, after which it should be submitted to the Senior Manager: Corporate Services for final approval.
- The ICT Manager will decide whether or not it is necessary to notify the users of the affected application of the scheduled patching of the application.

8.7 DEPLOYMENT

- When a patch has been successfully certified as ready for deployment and the necessary approval obtained, the patch should be deployed within the timeframes set out in the table above in point 4.3, taking into account the results of risk assessment and testing.
- In all instances, testing, either pre- or post-implementation, must be performed and documented for auditing and tracking purposes.

8.7.1 Windows Server Update Services (WSUS) configurations

- Group Policy – WSUS client setting are deployed using group policy
- A GPO created is named WSUS Client Settings and linked to the Domain level.



The group policy:

- Enables Windows Updates, specifies that updates will automatically be downloaded to clients, but prompt them to install the updates.
- Directs the windows clients to update from server.

WSUS Client Settings

Data collected on: 3/24/2017 11:00:46 AM

Computer Configuration (Enabled)

Policies

Administrative Templates

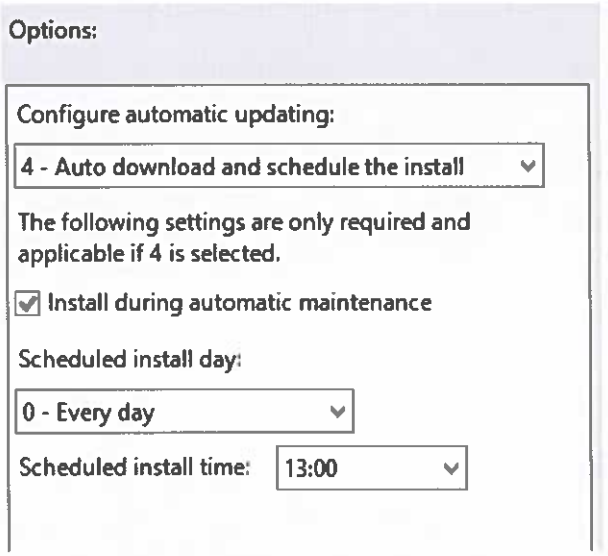
Policy definitions (ADMX files) retrieved from the local computer

Windows Components/Windows Update

Policy	Setting	Comment
Allow non-administrators to receive update notifications	Enabled	
Configure Automatic Updates	Enabled	
Configure automatic updating:	3 - Auto download and notify for install	
The following settings are only required and applicable if 4 is selected.		
Install during automatic maintenance	Disabled	
Scheduled install day:	0 - Every day	
Scheduled install time:	00:00	

Policy	Setting	Comment
Specify intranet Microsoft update service location	Enabled	

All computers that are joined to the domain will automatically get these settings and will connect to the WSUS server.

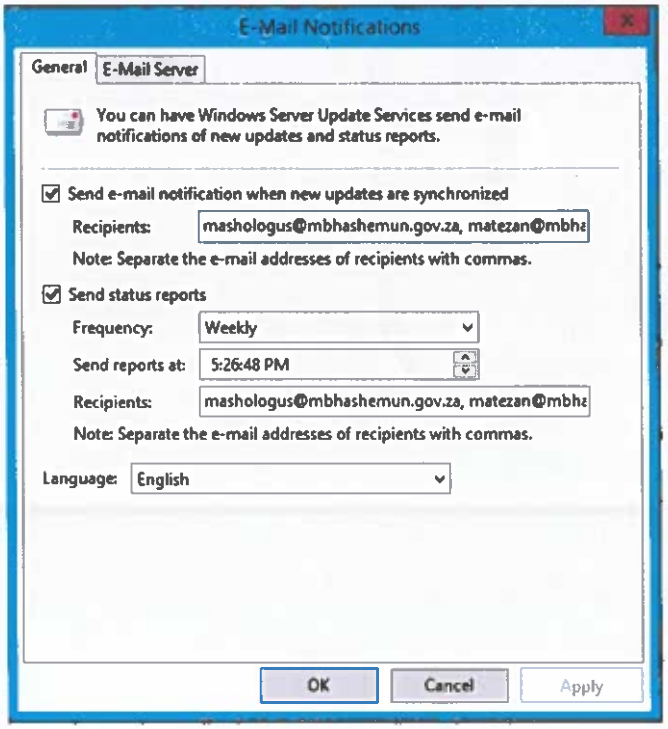


Firewall Settings

Fortigate is configured to BLOCK updates from Windows Update (internet) from the LAN subnets; a special policy is created to ALLOW updates from the WSUS server.

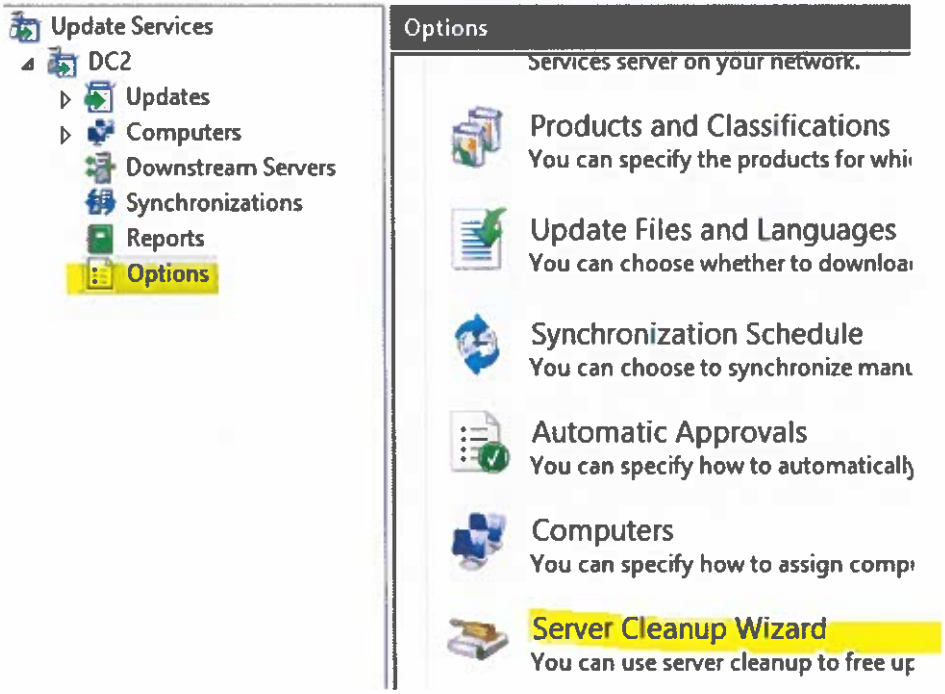
Reporting

Email notifications to be sent to System Administrator and Manager ICT, when updates are received, and a weekly status report.

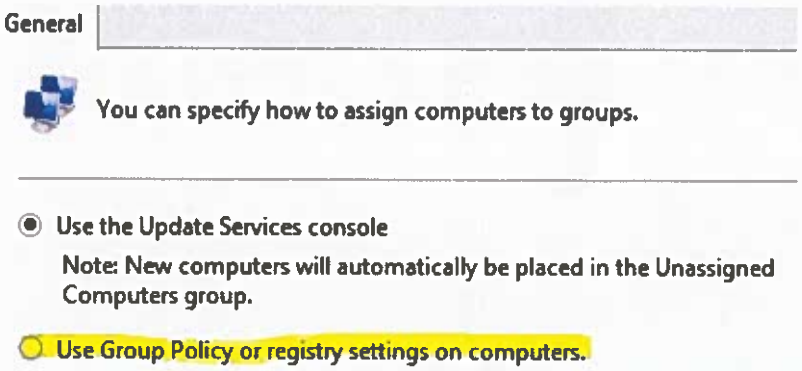


Regular Maintenance

- Check computers and updates on a regular (daily?) basis.
- Run the WSUS cleanup wizard every 3-4 months.



Computers configurations to be grouped according to Group Policy:



8.8 AUDITING, ASSESSMENT AND VERIFICATION

- A post-implementation review should be conducted to identify issues such as installation problems, process weaknesses and lessons learned.
- The results of the post-implementation of the patch should be documented for audit and tracking purposes.

9. IMPLEMENTATION

2023/2024

10. REVIEWAL

Annually