FETAKGOMO TUBATSE

LOCAL MUNICIPALITY

Patch Management Policy

Council Resolution OC148/2018

Document Control Information:

Date:	21/5/18
Master Tracking Name	Patch Management Policy
Master Tracking Reference	
Owning Service	Fetakgomo Tubatse Local Municipality
Issue:	1

Approvals:

Authors:	P.O.S Marome
Recommended By:	IT Steering Committee
Approved By:	Municipal Audit Committee

Document Control

Author	Version	Date Issued	Changes	Approval
P. Marome	0.1	04/09/17	Creation of document	
M.I Phasha	0.2	27/09/17	QA of V0.1 addition of CAB measures.	
Audit Committee	1.0	May 2018	Format and added in Third Party Suppliers	Audit Committee
Next review due: July 2020				

Contents

1. Introduction

Fetakgomo Tubatse Local municipality has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third parties.

The Municipality has an obligation to provide appropriate and adequate protection of all IT estate whether it is IT systems on premise, in the Cloud or systems and services supplied by third parties.

Effective implementation of this policy reduces the likelihood of compromise which may come from a malicious threat actor or threat source.

2. Purpose

This document describes the requirements for maintaining up-to-date operating system security patches and software version levels on all the Municipality owned estate and services supplied by third parties.

3. Definitions

The term IT systems includes:

Workstations

Servers (physical and

virtual) Firmware

Networks (including hardwired, Wi-Fi, switches, routers

etc.) Hardware

Software (databases, platforms etc.)

Applications (including mobile apps)

Cloud Services

4. Scope

This policy applies to:

Workstations, servers, networks, hardware devices, software and applications owned

by the Fetakgomo Tubatse Local Municipality and managed by IT Unit. This includes third parties supporting Municipal IT systems.

Systems that contain Municipal or customer data owned or managed by IT Unit regardless of location. Again, this includes third party suppliers.

CCTV systems where recordings are backed up to the Municipality's networks. Point of payment terminals using Municipality's networks.

Third party suppliers of IT systems as defined in Section 3.

5. Policy

Municipality controls:

All IT systems (as defined in section 3), either owned by the Fetakgomo Tubatse Local Municipality or those in the process of being developed and supported by third parties, must be manufacturer supported and have up-to-date and security patched operating systems and application software.

Security patches must be installed to protect the assets from known vulnerabilities.

Any patches categorised as 'Critical' or 'High risk' by the vendor must be installed within 14 days of release from the operating system or application vendor unless prevented by Municipality IT Change Control and procedures.

Where Change control procedures prevent the installation of 'Critical' or 'High risk' security patches within 14 days a temporary means of mitigation will be applied to reduce the risk.

- **Workstations**
  - All desktops and laptops that are managed by Municipal IT unit must meet the Laptop and Workstation Build Policy minimum requirements in build and setup. Any exceptions shall be documented and reported to IT Manager or Risk Management Officer responsible for Security and Compliance.
- **Servers**

- Servers must comply with the recommended minimum requirements that are specified by IT Unit which includes the default operating system level, service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to Municipal IT Manager for Security and Compliance.

Third Party Suppliers:

Security patches must be up-to-date for IT systems which are being designed and delivered by third party suppliers prior to going operational. Third party suppliers much be prepared to provide evidence of up-to-date patching before IT systems are accepted into service and thus become operational.

Once the IT systems are operational the following patching timescales apply:

Critical or High Risk vulnerabilities – 14 calendar

days Medium – 21 calendar days

Low – 28 calendar days

6. Roles and Responsibilities

Municipal IT Unit.

- Will manage the patching needs for the Windows, Apple Mac OS and Linux estate that is connected to the Fetakgomo Tubatse Local Municipality domain.
- Responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management.

ICT Steering Committee.

- Responsible for approving the Quarterly and emergency patch management deployment requests.

End User.

- The end user has a responsibility to ensure that patches are installed and the machine is rebooted when required. Any problems must be reported to Municipal IT Unit.

Third Party Suppliers

- Will ensure security patches must be up-to-date for IT systems which are being designed and delivered by third party suppliers prior to going operational.

- Once the IT systems are operational third party suppliers must ensure vulnerability patching is carried out as stipulated in Section 5 – Policy. Where this is not possible, this must be escalated to the IT Manager and Risk Officer responsible for Security and Compliance.

7. Monitoring and Reporting

Those with patching roles as detailed in section 6 above are required to compile and maintain reporting metrics that summarise the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Risk Management Team and Internal Audit upon request.

8. Policy Review and Maintenance

The Policy will be reviewed and updated after 24 months, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

9. For advice

Please contact either the IT Manager or Risk Management Office responsible for Security and Compliance. Queries can be emailed to maromep@tubatse.gov.za