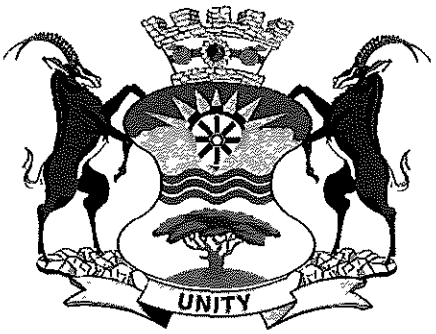
Rustenburg Local Municipality



Patch Management Policy

(Version 1)

Document Control Information:

Document Control

Author	Version	Date Issued	Changes	Approval
P. Marome	0.1	06/08/2020	Creation of document	
Next review due: September 2022				

Contents

1. Introduction

1. Rustenburg 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.

1.2 The Municipality has an obligation to provide appropriate and adequate protection of all IT assets whether they are IT systems on the municipal premises, in the Cloud or systems and services supplied by third parties.

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

2. Purpose

2 1 This document describes the requirements for maintaining up-to-date operating system security patches and software version levels on all the Municipal owned assets and services supplied by third parties

3. Definitions

3 1 The term IT systems includes·

a) Workstations

b) Servers (physical and virtual) Firmware

c) Networks (including hardwired, Wi-Fi, switches, routers etc.)

d) Hardware

e) Software (databases, platforms etc)

f) Applications (including mobile apps)

g) Cloud Services

4. Scope

This policy applies to·

4 1 Workstations, servers, networks, hardware devices, software and applications owned by the Rustenburg Local Municipality and managed by IT Unit This includes third parties supporting the Municipality's IT systems.

4.2 Systems that contain Municipality or customer data owned or managed by Municipal IT Unit regardless of location Again, this includes third party suppliers CCTV systems where recordings are backed up to the Municipal's networks

4 3 Point of payment terminals using Municipality's networks.

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

5. Policy

5.1 Municipal Controls:

5 1 1 All IT systems (as defined in section 3), either owned by the 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

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

5 1.3 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 (IT STECO – IT Steering Committee) procedures.

5 1 4 Where IT STECO 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

5.2 Workstations

5 2.1 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 Municipal IT Unit Manager or Director' Corporate Support Service for IT internal controls and Compliance purpose.

5.3 Servers

5 3 1 Servers must comply with the recommended minimum requirements that are specified by Municipality IT Unit which includes the default operating system level, service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to IT Unit Manager.

5.4 Third Party Suppliers:

5 4 1 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

5 4 2 Once the IT systems are operational the following patching timescales apply.

5 4 2.1 Critical or High Risk vulnerabilities – 14 calendar days

5 4 2 2 Medium – 21 calendar days

5 4 2 3 Low – 28 calendar days

6. Roles and Responsibilities

6.1 Municipal IT Unit

a) Will manage the patching needs for the Windows, Apple Mac OS and Linux estate that is connected to the Municipality domain
b) 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

6.2 Director: Corporate Support Service

a) Responsible for approving the monthly and emergency patch management deployment requests

6.3 End User

a) 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 the IT Helpdesk

6.4 Third Party Suppliers

a) 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

b) 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

7. Monitoring and Reporting

7.1 Those with patching roles as detailed in section 6 above are required to compile and maintain reporting metrics that summarises 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 Cyber Security Team and Internal Audit upon request

8. Policy Review and Maintenance

8 1 The Policy will be reviewed and updated, bi-annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, policies, contractually obligations and best practice