EMAKHAZENI LOCAL MUNICIPALITY

INFORMATION AND COMMUNICATION TECHNOLOGY PATCH MANAGEMENT POLICY

Approved by Council on

Implementation Date

TABLE OF CONTENTS

POLICY AUTHORITIES

Compiled by	
Designation	
Signature	
Date	
Supported/Not Supported	
Designation	
Signature	
Date	
Approved/Not Approved	
Designation	Municipal Manager
Signature	
Date	
Effective Date	

POLICY CHANGE RECORD

The following changes have been made to this policy:

Version	Description of Change	Date Approved

1. MANDATE OF THE ICT DIRECTORATE

1.1 The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure, for the Municipality to realise its mandate.

2. OBJECTIVE OF THE POLICY

2.1 The objective of this policy is to proactively prevent the exploitation of vulnerabilities on computing and related devices.

2.2 All computers and network devices must be maintained at service provider supported levels and critical security patches must be applied in a timely manner consistent with an assessment of risk.

3. APPLICABILITY OF THE POLICY

3.1 This policy applies to employees, Contractors and Consultants assigned to work at the Municipality.

3.2 This policy covers all servers, workstations, network devices, operating systems, applications, and other information assets for which service providers provide system patches or security updates.

4. TERMS AND DEFINITIONS

Term	Definition
Network Devices	Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge or gateway.
Network Infrastructure	Includes servers, network devices, and any other back-office equipment.

Patch	A fix to a known problem with an OS or software program. For the purposes of this document, the term “patch” will include software updates.
OS	Operating System such as Windows, Mac, Linux.
Risk Assessment	An evaluation of the level of exposure to a vulnerability for which a patch has been issued.
Update	A new version of software providing enhanced functionality or bug fixes.

5. ACRONYMS

COBIT Control Objectives for Information Technology

ICT Information and Communication Technology

ICTSC Information and Communication Technology Steering Committee

ITIL Information Technology Infrastructure Library

6. REFERENCES

6.1 International Guidelines

Control Objectives for Information Technology (COBIT)

6.2 International Standards

Information Technology Infrastructure Library (ITIL)

ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

6.3 National Policy

Constitution of the Republic of South Africa, Act 108 of 1996

The Electronic Communications and Transactions (ECT) Act 25 of 2002

National Strategic Intelligence Act 2 of 2000 applicable for South Africa

Regulation of Interception of Communications Act 70 or 2002

State Information Technology Act 88 of 1998

7. POLICY STATEMENT

7.1 Many computer operating systems such as Microsoft Windows include software application programs that may contain security flaws. Occasionally, one of the flaws may permit an attacker to compromise a computer system.

7.2 A compromised computer system threatens the integrity of the network and all computers connected to that system. Almost all operating systems and many software applications have periodic security patches released by the vendor that need to be applied. Patches which are security related or critical in nature should be installed.

7.3 ICT will review, evaluate, and appropriately apply software patches in a timely manner. Should patches not be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of a risk assessment.

7.4 ICT will use automated tools, where available, to create a detailed list of all currently installed software on workstations, servers and other networked devices. A manual audit will be conducted on any system or device for which an automated tool is not available.

7.5 In the event that a system must be, reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading.

8. PROCEDURE

8.1 Automated tools will scan for available patches and patch levels, which will be reviewed in accordance with Microsoft's severity rating system – which provides single rating per vulnerability.

8.2 Manual scans and reviews will be conducted on systems for which automated tools are not available.

8.3 Risk assessment must be performed within 2 business days of the receipt of notification of critical patches or 2 business days following Microsoft Patch release. If a determination regarding the applicability of the patch or mitigating controls cannot be made in that time, a formal risk assessment process must be initiated.

8.4 Service provider supplied patch documentation will be reviewed in order to assure compatibility with all system components prior to being applied.

8.5 Where feasible, patches will be successfully tested on non-production systems installed with the majority of critical applications or services prior to being loaded on production systems.

8.6 Successful backups of mission critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified.

8.7 Patches will be applied during an authorised maintenance window in cases where the patch application will cause a service interruption for mission critical systems.

8.8 Patches will be prioritised and applied in accordance with Microsoft's severity rating system.

8.9 Reports will be generated for all system categories (servers, secure desktops or switches) indicating which devices have been patched. System reports help record the status of systems and provide continuity among administrators. The reports may be in paper or electronic form.

8.10 Patch Compliance Reports will be presented at ICT Risk meeting.

9. COMPLIANCE LEVELS

9.1 A compliance level refers to the percentage of computer devices that have been successfully patched or otherwise remediated such that they are no longer vulnerable.

9.2 Although a completely patched environment (100%) would be desirable, however, this does not take into account the reality of:

9.2.1 Users that own multiple computing devices (that are not always connected to the network or switched on).

9.2.2 Travelling employees with laptop computers who do not log into the Departmental network every day.

9.2.3 Computers being repaired or replaced by hardware service provider.

9.2.4 Computers that may or may not even still exist on the corporate network, yet still show up on recent network inventory reports.

9.2.5 Failed or over saturated Wide Area Network connections.

9.2.6 Computers registered in Active Directory that have been recycled or reimaged.

9.2.7 Virtual computer sessions that remain powered off for weeks or months at a time.

9.3 In light of the above considerations, ICT will observe compliance levels in the range between 85% and 97%.

10. ROLES AND RESPONSIBILITIES

10.1 The ICT Division shall:

10.1.1 Track newly discovered vulnerabilities and the associated patch compliance, as they apply to the network and computing devices in the Municipality. This role is also responsible for defining and publishing the Patch Management Policy, Disaster Recovery Plan, and target service levels.

10.1.2 Review Patch Compliance Reports and following up with Network Administrators when compliance is outside the established boundaries.

10.2 The Manager Corporate Services shall:

10.2.1 Approve the scheduled rollout of patches, as they pertain to changes made to the production network environment.

10.3 The ICT Manager or Network Administrator shall:

10.3.1 Test patches against the most commonly used workstation and server configurations in the environment.

10.3.2 Test patches for compatibility with business critical applications.

10.3.3 Manage, install and restart assigned servers to apply patches.

10.3.4 Review Windows Update Server Update Services (WSUS) health reports, monitoring the health of the Notification Server Infrastructure, ensuring that the patches are properly downloaded and configuration of the WSUS.

11. MONITORING

11.1 The Network Administrator or Information Security Officer (ISO) shall monitor security mailing lists, review vendor notifications and Web sites, and research specific public Web sites for the release of new patches. Monitoring will include, but not be limited to, the following:

- ✓ Scanning the Municipality's network to identify known vulnerabilities.

- ✓ Monitoring notifications, and Web sites of all vendors that have hardware or software operating on Municipality's network.

12. REVIEW AND EVALUATION

12.1 Once alerted to a new patch, The Network Administrator or ISO shall download and review the new patch hours of its release. The Network Administrator or ISO shall categorize the criticality of the patch according to the following:

- ✓ Emergency—an imminent threat to Emakhazeni Local Municipality's network
- ✓ Critical—targets a security vulnerability
- ✓ Not Critical—a standard patch release update not applicable to Emakhazeni Local Municipality's environment

Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing, and verifying.

13. RISK ASSESSMENT AND TESTING

13.1 The Network Administrator or ISO shall assess the effect of a patch to the corporate infrastructure prior to its deployment. The ICT division will also assess the affected patch for criticality relevant to each platform (e.g., servers, desktops, printers, etc.).

13.2 If Network Administrator or ISO categorizes a patch as an Emergency, the ICT Division considers it an imminent threat to the Municipality's network, therefore, *the Municipality* assumes greater risk by not implementing the patch than waiting to test it before implementing.

13.3 Patches deemed Critical or Not Critical will undergo testing for each affected platform before release for implementation. The Network Administrator or ISO will expedite testing for critical patches.

14. POLICY REVIEW

14.1 This policy shall be reviewed on an annual basis by the ICT Division to:

14.1.1 Determine if there have been changes in International, National or Internal references that may impact on this policy.

14.1.2 Determine if there are improvements or changes in the ICT process that should be reflected in this policy.