Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

PATCH MANAGEMENT POLICY AND PROCEDURES

Departmental Contact Details	
Physical Address	Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Cooperative Governance and Traditional Affairs Private Bag X0035 Bhisho 5605
Document Number	3
Document Name	Patch Management and Procedures
Custodian	Ms T.M. Luke
Designation	Director: Information Management Services
Component	DGITO
Telephone No.	040 940 7235
Cell Phone No.	076 141 1749
E-mail Address	tswakai.luke@eccogta.gov.za
Date Completed	30 November 2021
Date of Approval	
Date Last Amended	
Date For Next Review	December 2026
Related Policies	ICT Security Policy

SIGN OFF

Head of Department

This Policy has been recommended by Mr. AA Fani in my capacity as Head of Department of Department Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Policy.

The development of the policy on Patch Management to manage updates and fix any vulnerability on software applications on a computer and other technologies in the department.

Signed	
Designation	Mr. AA Fani, Head of Department: Cooperative Governance and Traditional Affairs
Date	07/03/2022

Executive Authority

The Department of Cooperative Governance and Traditional Affairs has an unprecedented opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to challenges of its people.

I therefore trust that guidance from this Patch management policy will contribute to the effective utilisation of the policy by the staff of the Department.

Signed	
Designation	MEC: Honourable XE Nqatha of Cooperative Governance and Traditional Affairs
Date	10/03/2022

1. Contents

1. PREAMBLE

The goal of vulnerability and patch Management is to ensure that the components forming part of information technology environment (hardware, software, and services) are up to date with the latest patches and updates.

Vulnerability and patch management is a vital role of preserving the components of the information technology resource availability to the end user. Without regular vulnerability testing and patching, the information technology environment could face risks which can be mitigated by regularly updating the software, firmware, and drivers. Poor patching can allow viruses and spyware to infect the network and allow security weaknesses to be exploited.

2. PURPOSE OF POLICY

This policy defines the procedures to be adopted for mitigating vulnerability and patch management.

3. 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.
WSUS	Windows Server Update Services
Update	A new version of software providing enhanced functionality or bug fixes.

4. APPLICATION AND SCOPE

4.1 This policy applies to all components of the information technology environment and includes: -

- Computers
- Servers
- Application Software
- Peripherals
- Routers and switches
- Databases
- Storage

4.2 All staff within the IT Department must understand and use this policy. IT staff is responsible for ensuring that the vulnerabilities within the IT environment are minimized and that the environment is kept patched up to date.

4.3 All users have a role to play and a contribution to make by ensuring that they allow patches to be deployed to their equipment.

5. LEGISLATIVE FRAMEWORK

I. Constitution of the Republic of South Africa, 1996

II. Minimum Information Security Standards (MISS)

III. State Information Technology Act (Act no 88 of 1998)

IV. Electronic Communications Security (Pty) Ltd Act 68 of 2002

V. Electronic Communications and Transactions Act of 2002

VI. Electronic Communications Act of 2005

VII. National Cybersecurity Policy Framework

VIII. Protection of Personal Information Act (POPI Act) of 2013

IX. Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002

6. RISKS

Without effective vulnerability and patch management there is the risk of the unavailability of systems. This can be caused by viruses and malware exploiting systems or by outdated software and drivers making instability to the systems.

7. POLICY STATEMENT

The department's IT environment will be patched according to this policy to minimize vulnerabilities.

7.1 IDENTIFYING PATCHES TO BE APPLIED

7.1.1 The department's anti-virus server will be configured to automatically download the latest virus and spyware definitions.

7.1.2 Windows patch management tools will be utilized to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.

7.1.3 Notifications of patches from application and database vendors will be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the supplier's website will be reviewed on a regular basis.

7.1.4 The websites of the suppliers of servers, PC's, tablets, printers, switches, routers, and peripherals will be reviewed to determine the availability of firmware patches.

7.1.5 Missing patches identified will be implemented as appropriate. Any weaknesses identified will be rectified.

7.1.6 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.

7.2 SECURITY PATCHING PROCEDURES

Policies and procedures shall be established and implemented for vulnerability and patch management. The process shall ensure that application, system, and network device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule
- Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

7.3 TYPES OF PATCHES

The following patches will be implemented on the different information technology environment types.

TYPE	PATCH
Server/ Computer	Drivers/ firmware
Operating system	Service packs
Application software	Service packs, feature packs
Routers and Switches	Firmware
Printers	Drivers, firmware
Scanners	Drivers, firmware
Anti-virus/ Anti spyware	Data file/ Virus definition update.

7.4 ROLES AND RESPONSIBILITIES

7.4.1 The IT Department will be responsible for identifying patches for the application systems which they administer.

7.4.2 IT Department will also be responsible for patch approval and ownership of all technical updates including operating systems, patches for workstations and servers, antivirus and antispyware, drivers of devices.

7.4.3 IT Department will use restore points where applicable to ensure rollback changes.

7.5 PATCHING SCHEDULE

The department's IT environment will be patched according to this schedule.

Workstations should be patched according to the schedule below

Time	Action	Product Used
Daily	Antivirus and spyware definitions configured to be installed as they are released.	Windows Defender Advanced Threat Protection
Daily	Microsoft critical updates and security updates configured to be approved for rollout as they are released.	WSUS and Microsoft Intune Management
Daily	Check that drivers are up to date.	WSUS

Windows Servers should be patched according to the schedule below.

Time	Action	Product Used
Daily	Antivirus and spyware definitions will be configured and installed as they are released. Critical Security patches installed.	Windows Defender Advanced Threat Protection
Daily	All outstanding patches.	WSUS and Microsoft Intune Management
Daily	Check that drivers are up to date.	WSUS

Printers, peripherals, switches and routers and storage should be patched according to the schedule below.

Time	Action
Annually	Check for new firmware updates

8. MONITORING

Network Administrator 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 departmental network to identify known vulnerabilities.
- Monitoring notifications, and Web sites of all vendors that have hardware or software operating on departmental network.

9. APPROVAL OF THE POLICY

The policy will be approved by Member of Executive Council (MEC) on the recommendation of the Head of Department.

10. REVIEW OF THE POLICY

This policy will be reviewed on every fifth year from the date of approval and/or when there are changes in legislation or the operating environment.

11. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (The date the policy takes effect	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.
2021		XE Nqatha (MEC)	Initial Policy Drafted