LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

Patch Management Policy

REF: 6/1/P

Reviewed Version 1.0 – 2017

Date of approval: 27 September 2017

Recommended by:

..... 2017-09-12

Head of Department **Date**

(Maisela RJ)

Approved by:

..... 27/09/2017

Hon MEC for Agriculture and Rural Development **Date**

(Mokaba-Phukwana, M)

Table of Contents

1. ACRONYMS AND ABBREVIATIONS

DPSA	Department of Public Service Administration
GITO	Governments Information Technology Office
HOD	Head of Department
ICT	Information Communication Technology
IT	Information Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Council

2. EXECUTIVE SUMMARY

This Policy is addressing all matters that are relevant to the integrity, protection and availability of information that is stored on the IT systems. It is specifying the various roles and responsibilities as well as discussing matters such as workstations, exceptions, enforcement and monitoring. All definitions are indicated to ensure clarity on all matters.

3. INTRODUCTION

The Limpopo Department of Agriculture and Rural Development is responsible for ensuring the confidentiality, integrity, and availability of data that is stored on its systems. The Department has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

This Policy is aligned to the Department of Public Service Administration (DPSA) ICT Security Guideline issued in May 2017.

4. PURPOSE AND OBJECTIVES OF THE POLICY

This document describes the Government Information Technology Office's (GITO) requirements for maintaining up-to-date operating system security patches on all Departmental owned and managed workstations and servers.

5. AUTHORITY OF THE POLICY

This policy is issued under the authority of both the Member of Executive Council (MEC) for Agriculture and Rural Development within Limpopo as the Executive Authority of the LDARD, and the Head of Department (HOD) as the Accounting Officer of LDARD in Limpopo.

6. LEGAL FRAMEWORK

- King III Code Chapter 5 – King III Governance of Information Technology
- ICT House of values
- CobIT 5 – a business framework for the governance and management of enterprise IT from ISACA
- DPSA's Corporate Governance for ICT (CGICT)
- DPSA's Governance for ICT (GICT)
- ISO 27001 - Information Security Management Systems Standard by the International Standards Organisation
- MISS – Minimum Information Security Standards

7. SCOPE OF APPLICATION

This policy applies to workstations or servers owned or managed by the LDARD. This includes systems that contain department or stakeholder data owned or managed by The Department regardless of location. The following systems have been categorized according to management:

i. System and Application servers managed by Application and Systems Specialists
ii. Microsoft Windows servers managed by the System Administrator, Domain Administrator and District Network Administrators.
iii. Workstations (desktops and laptops) managed by the System Administrator, Head Office Technicians and District Network Administrators.

8. DEFINITIONS

King III: The term used to refer to both "The King Report on Corporate Governance for South Africa (The Institute of Directors in Southern Africa), September 2009" and "The King Code on Corporate Governance for South Africa (The Institute of Directors in Southern Africa), September 2009".

COBIT 5: Is a framework that brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders.

Patch: A piece of software designed to fix problems with or update a computer program or its supporting data.

Trojan: A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions.

Virus: A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

Worm: A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

Department: Refers to the LDARD.

9. POLICY PRONOUNCEMENTS

Workstations and servers owned by the Department must have up-to-date (as defined by GITO's minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by the Department.

9.1 WORKSTATIONS

Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by The Department. Any exception to the policy must be documented and forwarded to the GITO for review. (See Section below on Exceptions.)

9.2 SERVERS

Servers must comply with the minimum baseline requirements that have been approved by the GITO. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Department's assets and the data that resides on the system. Any exception to the policy must be documented and forwarded to the GITO for review. (See Section below on Exceptions.)

9.3 ROLES AND RESPONSIBILITIES

i. Application and Systems Specialists: will manage the patching needs for the Application and System servers they manage.

ii. The System Administrator and Domain Administrator: will manage the patching needs for the Microsoft Windows servers on the network.

iii. Domain Administrator, System Administrator, IT Technicians and District Network Administrators: will manage the patching needs of all workstations on the network.

iv. Information Security: is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

v. The Change Management Board: is responsible for approving the monthly and emergency patch management deployment requests.

9.4 MONITORING AND REPORTING

Active patching teams noted in the Roles and Responsibility section within this Policy document are required to compile and maintain reporting metrics that summarize 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 Information Security and Internal Audit upon request.

9.5 ENFORCEMENT

Implementation and enforcement of this policy is ultimately the responsibility of all employees at The Department. Information Security and Internal Audit may conduct random assessments to ensure compliance with the Policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the Department's issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

9.6 EXCEPTIONS

Exceptions to the Patch Management Policy require formal documented approval from the GITO. Any servers or workstations that do not comply with the Policy must have an approved exception on file with the GITO. Please refer to the GITO or Information Security Officer for details on filing exceptions.

10. DEFAULT

Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

Non-compliance and deviations from this Policy is not acceptable. Should it be necessary to deviate from this Framework, the written permission and motivation from the HOD will be required.

11. INCEPTION DATE

The inception date for this policy will be its date of approval – as indicated on the cover page of this Policy document.

12. TERMINATION AND REVIEW CONDITIONS

This Policy will be reviewed every three years (3) or as and when a need arise. Should the Policy still be in the review process by the time it lapses, an extension period is

applicable and the approved Policy remains valid until the reviewed version is approved.

13. ENQUIRIES AND REPORTING

Any enquiries with regard to any matter relating to this policy or exemption requests shall be directed to the GITO Service Desk at the LDARD: 015 294 3000.

GITO is responsible for the timeous review, circulation, advocacy, availability and feed-back regarding this Policy document. GITO is also responsible for reporting towards oversight bodies in the event of enquiries with regards to this Policy document.

Recommended by:

.....

Head of Department

(Maisela, RJ)

2017-09-12

.....

Date

Approved by:

.....

Hon MEC for Agriculture and Rural Development

Mapula Mokaba-Phukwana (MPL)

27/09/2017

.....

Date