



DEPARTMENT OF AGRICULTURE

**Patch Management Policy**

REF: 6/1/P

Version 1.0; 2015

Date of approval: 10 April 2015

Recommended by:

2015-03-24

Head of Department

Date

(Maisela, RJ)

Approved by:

2015/12/10

Hon MEC for Agriculture

Date

(Matshoge, BAJ)

<b>Table of Contents</b>	<b>Page</b>
1. Acronyms and abbreviations	1
2. Executive summary	2
3. Introduction	2
4. Purpose and objectives of the Policy	2
5. Authority of the Policy	2
6. Legal Framework	2
7. Scope of application	3
8. Definitions	3
9. Policy Pronouncements	4
9.1 Workstations	4
9.2 Servers	4
9.3 Roles and responsibilities	4
9.4 Monitoring and reporting	4
9.5 Enforcement	5
9.6 Exceptions	5
10. Default	5
11. Inception date	5
12. Termination and review conditions	5
13. Enquiries	5

## 1. Acronyms and abbreviations

<b>DPSA</b>	Department of Public Service Administration
<b>GITO</b>	Governments Information Technology Office
<b>HOD</b>	Head of Department
<b>ICT</b>	Information Communication Technology
<b>IT</b>	Information Technology
<b>LDA</b>	Limpopo Department of Agriculture
<b>MEC</b>	Member of Executive Committee

## **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 discuss matters such as workstations, exceptions, enforcement and monitoring. All definitions are indicated to ensure clarity on all matters.

## **3. Introduction**

Limpopo Department of Agriculture (herein The Department) 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.

## **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 Department owned and managed workstations and servers.

## **5. Authority of the policy**

This policy is issued under the authority of both the Member of Executive (MEC) for Agriculture as the Executive Authority of the LDA, and the Head of Department (HOD) as the Accounting Officer of LDA 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 Department. This includes systems that contain department or stakeholder data owned or managed by The Department of 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** **C**ontrol **O**bjectives for **I**nformation and Related **T**echnology **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.

## 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 9.6 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 9.6 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 9.3* 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 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 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**

Breach of policy and sanctions are as defined in *section 9.8 of the Information Security Policy*.

### **11. Inception date**

The inception date for this policy will be its date of approval.

### **12. Termination and review conditions**

The Department will conduct a review of the policy at least after every twenty-four (24) months or following any significant security incidents, changes to the South African legislation or changes to the Department's business requirement or structure.

### **13. Enquiries**

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

Recommended:

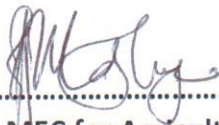


.....  
Head of Department  
(Maisela, RJ)

2015-03-24

.....  
Date

Approved:



.....  
Hon MEC for Agriculture  
(Matshoge, BAJ)

2015-04-10

.....  
Date