




**DEPARTMENT OF AGRICULTURE**

**Patch Management Policy**

Ref: 6/1/P


Date of effect:

Recommended/ ~~Not Recommended~~

  
\_\_\_\_\_  
Head of Department

23/02/2012  
Date

Approved/ ~~Not Approved~~

  
\_\_\_\_\_  
MEC for Agriculture:

27/02/2012  
Date

Comments:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## Table of Contents

<b>1</b>	<b>ACRONYMS &amp; DEFINITIONS .....</b>	<b>3</b>
<b>2</b>	<b>PURPOSE.....</b>	<b>3</b>
<b>3</b>	<b>LEGAL FRAMEWORK.....</b>	<b>3</b>
<b>4</b>	<b>OBJECTIVE OF THE POLICY .....</b>	<b>4</b>
<b>5</b>	<b>SCOPE OF APPLICATION.....</b>	<b>4</b>
<b>6</b>	<b>POLICY STATEMENTS .....</b>	<b>4</b>
6.1	BACKGROUND.....	4
6.2	OPERATIONAL GUIDELINES.....	5
6.3	TECHNICAL GUIDELINE.....	5
6.4	APPROVAL PROCESS.....	5
6.5	DEPLOYMENT.....	6
6.6	TESTING.....	6
6.7	AUDITING AND MONITORING .....	7
6.8	CONTINGENCY PLANNING .....	7
6.9	INCIDENT RESPONSE AND REPORTING .....	7
6.10	COMMUNICATIONS.....	7
6.11	ROLES AND RESPONSIBILITIES.....	8
6.12	SECURITY VIOLATION AND DISCIPLINARY MEASURES .....	8
<b>7</b>	<b>POLICY REVIEW .....</b>	<b>8</b>
<b>8</b>	<b>ENDORSEMENT .....</b>	<b>9</b>

# 1 ACRONYMS & DEFINITIONS

<b>AD</b>	Active Directory
<b>CA</b>	Computer Associates
<b>GITO</b>	Government Information Technology Office
<b>IP</b>	Internet Protocol
<b>IT</b>	Information Technology
<b>LDA</b>	Limpopo Department of Agriculture
<b>SITA</b>	State Information Technology Agency
<b>Backup media</b>	Media you back up data on to, for example laptop, tape, CD-ROM, etc.
<b>CA agent</b>	Software installed on LDA laptops, desktops and servers for compliance and management services.
<b>Change Advisory Board</b>	Group of people that approve requested changes and assist in the assessment and prioritization of changes.
<b>Domain</b>	Identification string that defines a realm of administrative autonomy, authority, or control in the Internet
<b>Information asset</b>	Refers to electronic data, information, business application systems, operating systems, computer equipment and other IT infrastructure.
<b>Server</b>	Is a physical computer dedicated to running one or more such service to serve the needs of users of the other computers on the network

## 2 PURPOSE

The purpose of this policy is to preserve the confidentiality, integrity and availability of LDA electronic information.

## 3 LEGAL FRAMEWORK

- a) SITA Act, of 1998
- b) Public Service Act, No 103 of 1994



## 4 OBJECTIVE OF THE POLICY

The following are the main objectives of this policy:

- To ensure all LDA IT systems do not pose an unmanaged security risk for the organisation, by ensuring applicable and required security patches and software updates for LDA IT systems are applied in a timely and effective manner.
- To define organisation standards for auditing, reporting, communication, and contingency planning with regards to the management of security patches and software updates.

## 5 SCOPE OF APPLICATION

This policy applies to employees, contractors, consultants, temporaries, and other workers at LDA including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by LDA such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

## 6 POLICY STATEMENTS

### 6.1 BACKGROUND

Many computer operating systems such as Microsoft Windows, Linux, Mac OS and others include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the network and all computers connected to it. Almost all operating systems and many software applications have periodic security patches and software updates released by the vendor that need to be applied. Patches which are security related or critical in nature should be installed.

- In the event that a critical or security patch cannot be centrally deployed, it must be installed in a timely manner using the best resources available. In the case of non-Microsoft desktop operating systems where a centralized deployment is not available then installation should occur in a timely manner by a member of LDA IT Department, or the end user.
- Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing or tampering with patch management protections and/or software constitutes a violation of policy.

## 6.2 OPERATIONAL GUIDELINES

- LDA IT Department must subscribe to Security Bulletin email distribution list of technologies deployed in the organization environment.

## 6.3 TECHNICAL GUIDELINE

- Current patches for all LDA vendor supported products must be maintained.
- LDA IT Department must at a minimum, audit all networked computers monthly to determine the need for security patches and software release. Automatic scanning systems, administered from central sites, are superior to manual patching methods. It must be possible to define scans by:
  - IP ranges
  - Domain/AD
- It must be possible to automatically deploy patches from central sites following the same criteria described for scanning.
- If administrative rights to a computer are necessary requirements for a selected automated patch management system then local creation of an assured access to that account are conditions for continued attachment of that computer to a LDA network. Required administrative accounts will follow minimal password standards for authentication. Default passwords will not be allowed.
- Automated scanning and deployment (patch management) systems must also be able to provide lists of:
  - Missing Patches and/or Service Packs.
  - Operating System Versions.
  - Patches that were successfully applied.
  - Patches that could not be applied.
- The patch management product employed must store all information in a structured database.

## 6.4 APPROVAL PROCESS

Since a security patch may cause an application to malfunction, LDA IT Manager/ISO should proactively announce the deployment of a patch (es) to LDA Change Advisory Board. It is the responsibility of application owners to identify any problem(s) with a patch (es) and to notify the LDA IT Manager/ISO of



the problem(s). It is also the responsibility of application owners to resolve this incompatibility with the application's maker. If the maker cannot resolve the incompatibility, the risk incurred by not patching the computer(s) in question must be weighed against the risk of not running the application. LDA IT Manager/ISO and the application owner should evaluate the options taking into consideration the nature of the vulnerability, the likelihood of its exploitation and the impact to operations of application malfunction. If they determine that the patch in question should not be deployed, this decision must be communicated to the GITO.

## 6.5 DEPLOYMENT

The patch deployment window refers to the allowable timeframe for the identification, analysing and distribution of security patches within the LDA environment.

Patch Rating	Analysis	Testing	Deployment	Total
Critical (Emergency)	0.5 days	0.5 days	1 day	2 days
Critical/Important	1 day	1 day	1 day	3 days
Medium/ Moderate	1 day	1 day	1 day	3 days
Low	1 day	2 days	2 days	5 days

A roaming workstation must have Windows Automatic Updates and CA agent configured to automatically download and install patches when it physically connects to LDA network.

## 6.6 TESTING

- Patches shall be tested on non-production systems prior to installation on all production systems.
- It is the responsibility of application owners to identify any problem(s) with a patch (es) and to notify the IT manager of the problem(s).
- It is also the responsibility of application owners to resolve this incompatibility with the application's manufacturer.
- If the manufacturer cannot resolve the incompatibility, the risk incurred by not patching the computer(s) in question must be weighed against the risk of not running the application.

- If they determine that the patch in question should not be deployed, this decision must be communicated to LDA Change Advisory Board.

## **6.7 AUDITING AND MONITORING**

- Post-patch audit scans must occur within 1 week for all critical security patches.
- Regular or pre-patch network-wide audit scans must be performed at least monthly.

## **6.8 CONTINGENCY PLANNING**

### **6.8.1 System Failure**

- In the event that a critical patch cannot be centrally deployed, it must be installed manually.
- One or more alternate central console server administrators must be designated and trained so that in the event the primary administrator or LDA IT Manager/ISO is not available the patch and audit processes can proceed normally.

## **6.9 INCIDENT RESPONSE AND REPORTING**

### **6.9.1 Outbreak Management**

LDA IT department will take reasonable and appropriate measures to defend networking functions during malicious attacks. All security incidents shall be reported or escalated and resolved in accordance with **LDA Information Security Incident Management Policy**.

## **6.10 COMMUNICATIONS**

### **6.10.1 General communications**

Digital communications (email and web) must be distributed at all levels during patch management process.



## 6.11 ROLES AND RESPONSIBILITIES

Issue	Person Responsible	Alternate
Has overall responsibility for adherence to policy	LDA GITO	LDA IT Manager
Has the responsibility for implementation and adherence to the policy	LDA ISO	LDA IT Manager

## 6.12 SECURITY VIOLATION AND DISCIPLINARY MEASURES

- Any attempts to bypass security controls or to obtain unauthorised access or to make unauthorised use of a user account belonging to someone else shall be considered a security violation.
- The use of LDA's information assets for purpose other than for authorised business purposes shall be considered a security violation.
- The use of LDA information assets for any unauthorised or illegal activity shall be considered a security violation
- Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure shall be considered a security violation.
- Any act (or failure to act) that results in sensitive or business critical information being disclosed to an unauthorised person shall be considered a security violation.
- Any act (or failure to act) that results in sensitive or business critical information being modified or destroyed such that the LDA or any of its branches / sub branches is adversely impacted shall be considered a security violation.
- Any breach of this policy or any of its related documents shall be considered a security violation.
- Any person charged with a security violation shall face disciplinary action.
- All information abuses and security breaches should be reported to the Information Security Officer.

## 7 POLICY REVIEW

The policy shall be reviewed after every year or as and when the need arise with the permissions from the MEC.



