



LIMPOPO  
PROVINCIAL GOVERNMENT  
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF  
AGRICULTURE AND RURAL DEVELOPMENT

**Antivirus Management Policy**

Ref: 6/1/P

Date of approval: 13 June 2016

Recommended by:

1 M Maisela

Maisela, RJ

(Head of Department)

03/06/2016

Date

Approved by:

Matshoge

Matshoge, BAJ

(Hon MEC for Agriculture and  
Rural Development)

13/06/16

Date

Table of Contents	Page
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	3
7. Scope of application	3
8. Definitions	3
9. Policy pronouncements	3
9.1 Antivirus management: Roles and Responsibilities Matrix	3
9.2 Standard Operating Environment	4
9.3 Configuration Management Database	4
9.4 Antivirus Management Key Tiers	5
9.5 Auditing and Monitoring	7
9.6 Communications	7
9.7 Roles and Responsibilities	7
10. Default	8
11. Inception date	8
12. Termination and review conditions	8
13. Enquiries	9

## 1. Acronyms and abbreviations

<b>GITO:</b>	Government Information Technology Office
<b>HOD:</b>	Head of Department
<b>IT:</b>	Information Technology
<b>LDARD:</b>	Limpopo Department of Agriculture and Rural Development
<b>MEC:</b>	Member of Executive Council
<b>SITA:</b>	State Information Technology Agency
<b>SMTP:</b>	Simple Mail Transfer Protocol

## **2. Executive summary**

The IT policy on Antivirus Management is a policy that intends to cover all matters relevant to the management of the LDARD Antivirus System. It provides a detailed description of roles and responsibilities and monitoring, the configuration management database, the standard operating environment, the antivirus management key tiers and other relevant matters – including security violation and disciplinary measures.

## **3. Introduction**

An Antivirus policy is key to any antivirus infrastructure and is the foundation on which the antivirus processes are developed.

An organisation may require an antivirus policy for different areas of the organisation. This policy is intended to ensure that every user that operates on the network knows what is required of them in protecting the infrastructure from malicious code.

## **4. Purpose and objectives of the policy**

The purpose of this policy is to document the key areas that LDARD will focus on when setting up Antivirus Management. It also points out some of the key configurations that should be considered when configuring Antivirus software.

The following are the main objectives of this policy:

- a) To provide detailed information on what each tier of Antivirus infrastructure is to achieve.
- b) To ensure that every person that connects to the environment knows the role they play in Antivirus Management.

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

This policy is issued under the custodianship of the Accounting Officer and the Honourable MEC for Agriculture and Rural Development in Limpopo.



## 6. Legal Framework

- 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

## 7. Scope of application

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

## 8. Definitions

<b>Virus:</b>	Computer program that is aimed at disrupting the normal functionality of a computer
<b>Antivirus:</b>	Computer program that prevents the virus to affect the computer and fixes any damage performed by the virus.
<b>LDARD:</b>	Limpopo Department of Agriculture and Rural Development
<b>SPAM:</b>	Unsolicited bulk email

## 9. Policy pronouncements

### 9.1 ANTIVIRUS MANAGEMENT: ROLES AND RESPONSIBILITIES MATRIX

Currently LDARD has standardized on Symantec Endpoint Protection for antivirus management. Symantec authorised resellers are appointed on ad-hoc basis for support or maintenance. Further an Information Security Officer was also appointed to assist LDARD with the implementation of information security program. Periodic assessment of the Symantic Anti-virus Software is being conducted every 12 months following the Gartner Quadrant guideline.

Below is the LDARD antivirus management roles and responsibilities matrix.

Virus Protection	Third Party	LDA
Monitoring of servers for virus infection	x	
Update virus definition files	x	
Update virus definitions files when a major outbreak is identified	x	
Rectification of virus infections on endpoints		x
Ensure that antivirus software on endpoints is not disabled		x
Ensure that there is proper communication to relevant stakeholders during virus outbreak		x
Report on major viruses outbreaks, detailing actions to resolve and prevent recurrence	x	
Ensure that all endpoint have antivirus agent installed		x
Ensure that all endpoints run and complete scans		x
Maintain subscription/maintenance service for all antivirus software	x	x

## 9.2 STANDARD OPERATING ENVIRONMENT

LDARD must ensure that it builds standard images for both servers and desktops/laptops. Standard Operating environment ensures that antivirus software is installed on every new computer that is put on the network.

## 9.3 CONFIGURATION MANAGEMENT DATABASE

To effectively manage antivirus infrastructure a configuration management database is required. The purpose of a configuration management database is to store all the information about the environment. With antivirus administration it is critical to know what services are running on all machines.

Advantages of configuration management database:

- c) Audit process is much faster.
- d) Speed up change management process.
- e) It allows you to restore a server to the correct baseline should it need to be rebuilt.

## 9.4 ANTIVIRUS MANAGEMENT KEY TIERS

The following are key tiers that need to be considered.

### 9.4.1 Management Tier

The first tier is the Management tier. From this tier the entire antivirus infrastructure is managed, updates can be controlled, reports can be run, outbreak tracking and infections are visible.

When implemented properly, this tier allows all the tiers of the network to be managed from one central point and allows automation of the tasks the antivirus administrator/specialist needs to perform.

### 9.4.2 Gateway Tier

From the Internet perspective the most common vector for a virus or worm to enter the network is via email (SMTP) followed by http traffic therefore it is critical that antivirus and SPAM management solution is implemented in this tier.

Security patching of any gateway server is also critical due to their proximity to the internet.

### 9.4.3 Internal Email System

The next tier down from the gateway tier is the internal email system. Running an antivirus service on the internal email system is critical as email is the most common vector for spreading of viruses and worms on an internal network.

Another point to remember when implementing antivirus software on email servers is to ensure that the operating system is protected. Most antivirus vendors have separate product for scanning and cleaning emails but this product will not protect the operating system itself so it is important to install the software intended for this task.

Operating system scanner must be configured to ignore some files and directories, or possibly an entire partition or physical drive.



#### 9.4.4 File and Print Servers, Plus Others

This category covers all the servers outside of the gateways and internal email servers discussed above. Some example servers would be: file servers, print servers, domain controllers, and database hosts. This is also the tier that hosts a company's most critical data and hence requires protection.

When configuring antivirus software on a server in this category there are some things you need to take into consideration such as:

- a) When should a schedule scan run
- b) What is impact of real time scanning and should it be on.
- c) What files, file types, directories, or drives should be excluded from scan.
- d) How infected files should be handled.

It is not uncommon for a critical or business related file to be infected with the virus and if this does occur you may not want to delete the file, especially if it has not been backed up. In order to have the ability to try and clean the file manually you may want to configure the antivirus software to first try and clean the file and then, as a backup. If the file can't be cleaned you may want to quarantine it rather than delete it.

#### 9.4.5 Desktop Tier

This is by far the hardest tier to manage and the main reason for this is that there are usually a large number of clients.

The configuration of an antivirus desktop client should require as little input from the user as possible.

The following must be prevented from end-users:

- a) Ability to disable the antivirus service.
- b) Ability to disable or cancel a scheduled scan.
- c) Ability to disable real time scanning.
- d) Ability to uninstall antivirus agent.

When configuring the desktop scheduled scan time, it is important to remember that when a scheduled scan is running there will be considerable performance impact to the machine. Because of the impact to performance most users, due to their lack of knowledge, will attempt to stop the scan. To minimise the impact that scanning will have on the users' productivity, you should look at running



the scan when it is going to least impact the user. This would usually be at night when the user is not at work. One problem with running a scan at night, or outside of business hours, is that a lot of users will shut their machine down and hence it will not get scanned, or, due to the smarts in the software it will get scanned when the machine is next turned on.

User awareness and training is critical in minimising security incidents associated with malware outbreaks.

## 9.5 AUDITING AND MONITORING

- a) LDARD Information Security Officer shall produce a weekly report listing all viruses detected in the environment and how infections penetrated the environment.
- b) LDARD IT Department shall remediate infected machines accordingly.

## 9.6 COMMUNICATIONS

Digital communications (email and web) must be distributed at all levels during major virus outbreak.

## 9.7 ROLES AND RESPONSIBILITIES

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

## **10. Default**

No deviation from this policy is allowed. Should any deviation be needed, it will only be granted with the written approval of the Accounting Officer – after thorough investigation and motivation.

- 1) Any attempts to bypass security controls or to obtain unauthorized access or to make unauthorized use of a user account belonging to someone else shall be considered a security violation.
- 2) The use of LDARD's information assets for purpose other than for authorized business purposes shall be considered a security violation.
- 3) The use of LDARD information assets for any unauthorized or illegal activity shall be considered a security violation.
- 4) Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure shall be considered a security violation.
- 5) Any act (or failure to act) that results in sensitive or business critical information being disclosed to an unauthorized person shall be considered a security violation.
- 6) 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.
- 7) Any breach of this policy or any of its related documents shall be considered a security violation.
- 8) Any person charged with a security violation shall face disciplinary action.
- 9) All information abuses and security breaches should be reported to the Information Security Officer.

## **11. Inception date**

The date of approval (as indicated on the cover page of this policy) is also the date of inception.

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

This policy should be reviewed every 24 months (2 years) or as and when a need arise.

### 13. Enquiries

All enquiries regarding this policy should be directed towards:

The Director: IT

Limpopo Department of Agriculture and Rural Development

PO Box 9487

POLOKWANE

0700

Tel: 015 294 3000

E-mail: [ITHelpDesk@agric.limpopo.gov.za](mailto:ITHelpDesk@agric.limpopo.gov.za)

**Recommended by:**



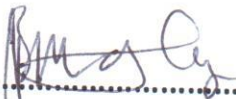
Maisela, RJ

(Head of Department)

03/06/2016

Date

**Approved by:**



Matshoge, BAJ

(Hon MEC for Agriculture and Rural Development)

03/06/2016

Date