LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF AGRICULTURE

Antivirus Management Policy

Ref: 6/1/P

Date of effect:

Recommended/ ~~Not Recommended~~

Head of Department

23/02/12
Date

Approved/ ~~Not Approved~~

MEC for Agriculture:

24/02/2012
Date

Comments:

Table of Contents

1 ACRONYMS & DEFINITIONS

GITO:	Government Information Technology Office
IT:	Information Technology
LDA:	Limpopo Department of Agriculture
SITA:	State Information Technology Agency
SMTP:	Simple Mail Transfer Protocol
SPAM:	Unsolicited bulk email

2 PURPOSE

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

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

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

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.

6.2 ANTIVIRUS MANAGEMENT: ROLES AND RESPONSIBILITIES MATRIX

Currently LDA 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 LDA with the implementation of information security program.

Below is the LDA 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

6.3 Standard Operating Environment

LDA 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.

6.4 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:

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

6.5 Antivirus Management Key Tiers

The following are key tiers that need to be considered.

6.5.1 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.

6.5.2 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.

6.5.3 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.

6.5.4 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:

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

6.5.5 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:

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

When configuring the desktop scheduled scan time, it is important toremember that when a scheduled scan is running there will be considerableperformance impact to the machine. Because of the impact to performancemost users, due to their lack of knowledge, will attempt to stop the scan. Tominimise the impact that scanning will have on the users' productivity, youshould look at running the scan when it is going to least impact the user. Thiswould usually be at night when the user is not at work. One problem withrunning a scan at night, or outside of business hours, is that a lot of users willshut their machine down and hence it will not get scanned, or, due to thesmarts 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.

6.6 Auditing and Monitoring

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

6.7 Some Good Practice

Regular pattern file updates are critical in the protection of the environment you manage. As a good practice LDA should try and ensure that there is more than one way a machine can receive new pattern files. For example, many antivirus clients can be set to download their pattern files independently from the vendor site as a backup to getting them from the management distribution point. This kind of backup is effective but it can cause an impact to the network in low bandwidth situations where normally the pattern file would be distributed outside of business hours. As this would only be a backup and pattern files would usually get updated in a controlled manner off the managed distribution point, a business decision could be made to accept occasional network impact to ensure the antivirus software is up to date.

Another good practice is to record when an antivirus update occurred. This isuseful information when generating a report as well as for tracking and monitoring.

Regular auditing of the antivirus infrastructure is a good idea. It is very easy when managing possibly thousands of server and tens of thousands of desktops to miss seeing machines that are failing to update or where the software has stopped working. It is also not common for servers or workstations to be put onto the network without antivirus software. Regular auditing will help remove these risks from the network. LDA should scan the network for machines without antivirus software; most vendors have a tool for doing this. LDA should also work through the management consoles and correct any machines that are not up to date. It can be a good idea to have a different person to the normal antivirus administrator run the audit so that there is a new set of eyes viewing the infrastructure.

6.8 Communications

General communications

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

6.9 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

6.10 Security violation and Disciplinary measures

- 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.
- The use of LDA's information assets for purpose other than for authorized business purposes shall be considered a security violation.
- The use of LDA information assets for any unauthorized 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 unauthorized 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.

8 ENDORSEMENT

Activity	Name	Signature	Date
Adoption	LDA IT Steering Committee		2012/02/09
Authorization	LDA GITO: Kgaogelo Mohlala		2012/02/09