



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

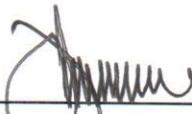
DEPARTMENT OF AGRICULTURE

Network Security Policy

Ref: 6/1/P

Date of effect:

Recommended/ ~~Not Recommended~~




Head of Department

23/02/12

Date

Approved/ Not Approved



MEC for Agriculture:

27/02/2012

Date

Comments:

Table of Contents

REF: 6/1/P.....	1
DATE OF EFFECT:.....	1
1 ACRONYMS & DEFINITIONS	3
2 PURPOSE.....	3
3 LEGAL FRAMEWORK	3
4 OBJECTIVE OF THE POLICY	3
5 SCOPE OF APPLICATION	4
6 POLICY STATEMENTS	4
6.1 BACKGROUND.....	4
6.2 PRINCIPLES – WIRED NETWORK CONNECTIVITY.....	4
6.2.1 Network Access Point.....	4
6.2.2 Network Perimeter Security	5
6.2.3 Firewalls.....	5
6.3 PRINCIPLES – GENERAL	6
6.3.1 Documentation	6
6.3.2 Change Control.....	7
6.3.3 Access	7
6.3.4 Incident Management	7
6.3.5 Contingency Planning	7
6.3.6 Malicious Software	7
6.3.7 Backup	7
6.3.8 Firewall Backup	7
6.4 ROLES AND RESPONSIBILITIES.....	7
6.5 SECURITY VIOLATION AND DISCIPLINARY MEASURES.....	8
7 POLICY REVIEW	8
8 REFERENCES	8
9 ENDORSEMENT	9

1 ACRONYMS & DEFINITIONS

GITO:	Government Information Technology Office
IT:	Information Technology
LDA:	Limpopo Department of Agriculture
SITA:	State Information Technology Agency
Mbps:	Megabit per second
SSID:	Service Set Identifier
WEP:	Wired Equivalent Privacy
Network Perimeter:	A network perimeter is the boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network.
Network Infrastructure:	A network infrastructure is an interconnected group of computer systems linked by the various parts of telecommunication architecture. Specifically, this infrastructure refers to the organization of its various parts and their configurations — from individual networked computers to routers, cables, wireless access points, switches, backbones, network protocols, and network access methodologies.

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 objective of this policy is to define network security principles and guidelines within LDA. These guidelines focus on vulnerabilities and controls as identified through:

- Connection to public networks (The Internet).
- User workstation.
- Network Infrastructure.

5 SCOPE OF APPLICATION

This policy is applicable to all users who make use of LDA's Network facilities. All users and staff to whom such facilities are provided are aware of the policy and act in accordance with them. The policy also applies to all temporary staff, contractors, service providers, or consultants. Any authorisation of access to, or use of the network facilities provided by LDA, shall be strictly subject to the provisions of this policy.

6 POLICY STATEMENTS

6.1 BACKGROUND

The adoption of modern networking technologies to integrate organizations with external entities electronically in recent years has transformed the concept of the physical and logical boundaries of an organization. Whilst it brings many benefits, such as rapid access to information, improved communications, reduced costs, increased collaboration with business partners, improved customer service and an unprecedented ability to conduct electronic commerce, it also presents organizations with a new set of security concerns.

This policy provides guidelines for operational procedures and responsibilities to ensure the correct and safe operation of the network.

6.2 PRINCIPLES – WIRED NETWORK CONNECTIVITY

The infrastructure supported shall be adequately protected thus ensuring the secure transportation of information across LDA's networks. Information shall be protected in accordance with business requirements. The following principles shall be adhered to, to comply with the policy requirements:

6.2.1 Network Access Point

The detail configuration and rules for all proposed new entry points into the LDA network, or proposed changes to existing entry points shall be documented. All existing entry points into the LDA network shall be identified and documented. The following information shall be included:

- The physical configuration
- Connection points
- The owner, or responsible official
- The administrator
- The purpose of the entry point

6.2.2 Network Perimeter Security

6.2.2.1 Approving Services

All proposed new entry points into the LDA network, or proposed changes to existing entry points are evaluated by the Security Manager for compliance with the LDA Security standards, as endorsed by the Security Forum.

All proposed new entry points into the LDA network, or proposed changes to existing entry points are approved by the Security Officer.

6.2.3 Firewalls

Firewalls are defined as security systems, which control and restrict both Internet connectivity and Internet services.

6.2.3.1 Dedicated Functionality

In some instances, systems such as routers may be functioning as though they are firewalls when in fact they are not formally known as firewalls. All LDA's systems playing the role of firewalls, whether or not they are formally called firewalls, must be managed according to the rules defined in this policy.

6.2.3.2 Logs

All changes to firewall/IPS configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity, which might be an indication of unauthorised usage or an attempt to compromise security measures, must also be logged. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

6.2.3.3 Intrusion Detection

All LDA's firewalls must include intrusion detection systems approved by the Security Forum. These intrusion detection systems must each be configured according to the specifications defined by the security standards.

6.2.3.4 External Connections

All inbound real-time Internet connections to LDA's internal networks and/or multi-user computer systems must pass through a firewall before users can reach a login banner.

6.2.3.5 Firewall/IPS Access and Privileges

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few individuals with a business need for these privileges. Unless permission from the Security Officer has been obtained, these privileges must be granted only to individuals who are full-time employees of LDA.

6.2.3.6 Network Management

Firewalls must be configured so that they are visible to internal network management systems. Firewalls must also be configured so that they permit the use of remote automatic auditing tools to be used by authorized LDA staff members.

6.3 PRINCIPLES – GENERAL

6.3.1 Documentation

Network operational procedures regarding all LDAs' common network facilities shall be documented and stored in a safe environment.

The minimum required to ensure this is:

- Roles and responsibilities of network staff
- Network restore procedures
- Network configuration settings for all critical equipment
- Firewall configuration settings
- Network diagrams clearly indicating logical connections and locations of the equipment on the network
- All of the above points needs to be reviewed on a regular basis as well as when a change in the network occurs.

6.3.2 Change Control

All changes and additions to LDA's network resources shall be in accordance with the LDA Change Control Policy.

6.3.3 Access

Access to network resources shall be managed by the LDA User Account Management Policy.

6.3.4 Incident Management

Network related security incidents and malfunctions shall be reported, escalated, resolved, monitored and communicated in accordance with the LDA Incident Management Policy.

6.3.5 Contingency Planning

Contingency plans must be developed which address the actions to be taken in the event of various problems including system compromise, system malfunction, and power outage.

6.3.6 Malicious Software

LDA network resources shall be protected against the introduction of malicious program code.

6.3.7 Backup

Essential network resources shall be backed-up and restored on a regular basis in accordance with the LDA Back-up Policy.

6.3.8 Firewall Backup

Current off-line backup copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to firewalls at all times. A permissible alternative to off-line copies involves on-line encrypted versions of these files. Either of these options will help to keep trusted copies away from intruders, but at the same time be immediately available to re-establish a secure and reliable computing environment.

6.4 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
---	---------	----------------

6.5 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 REFERENCES

- ISO 17799: Section 8.5.1
- CobIT: DS 5.1, PO2, PO3
- ITIL Book: Security Management

9 ENDORSEMENT

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