LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

Information and Communication Technology Network Security Policy

REF: 6/1/P

Reviewed Version 1.0 – 2017

Date of approval: 27 September 2017

Recommended by:

.....

Head of Department
(Maisela RJ)

2017-09-12
.....
Date

Approved by:

.....

Hon MEC for Agriculture and Rural Development
(Mokaba-Phukwana, M)

27/09/2017
.....
Date

Table of Contents

1. ACRONYMS AND ABBREVIATIONS

CD	Compact Disk
DPSA	Department of Public Service and Administration
DVD	Digital Video Disk
GITO	Government Information Technology Office
HOD	Head of Department
ICT	Information and Communication Technology
IDS	Intrusion Detection System
ITIL	Information Technology Infrastructure Library
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Council
SITA	State Information Technology Agency

2. EXECUTIVE SUMMARY

This Policy aims to ensure the correct and safe operation of the network and is applicable to all users accessing the networking devices.
This policy aims to define network security principles and guidelines.
The policy pronouncement is clear on all aspects regarding matters such as documentation, change control, access, incident management, contingency planning, malicious software, the backup as well as firewall backup.

Firewalls are discussed at length and include:

a) Dedicated functionality
b) Logs
c) Intrusion detection
d) External connections
e) Firewall/IPS Access and Privileges
f) Network management

All roles and responsibilities are clarified and the default is addressed in detail.

3. INTRODUCTION

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.

This Policy is aligned to the Department of Public Service and Administration (DPSA) ICT Security Guideline issued in May 2017.

4. PURPOSE AND OBJECTIVES OF THE POLICY

The purpose of this policy is to preserve the confidentiality, integrity and availability of Limpopo Department of Agriculture and Rural Development (LDARD) electronic information.

The objective of this policy is to define network security principles and guidelines within the LDARD. These guidelines focus on physical and logical access controls as identified through:
a) Connecting to networking devices.

b) Communication protocols.
c) Network monitoring.

5. AUTHORITY OF THE POLICY

This policy is issued under the authority of both the Member of Executive Council (MEC) as the Executive Authority of the LDARD, and the Head of Department (HOD) as the Accounting Officer.

6. LEGAL FRAMEWORK & REFERENCES

a) SITA Act, of 1998
b) Public Service Act, No 103 of 1994
c) International Standards Organisation (ISO) 17799: Section 8.5.1
d) COBIT: DS 5.1, PO2, PO3
e) ITIL Book: Security Management

Departmental Policies:
LDARD Records Management Policy

7. SCOPE OF APPLICATION

The information resources (the "Information Resources") included in the scope of the Information Security Policies are:

a) All data (as defined in Section 9 below) regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, compact disk (CD), Digital Versatile Disk (DVD), external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);
b) The Departmental computing hardware and software systems supported by GITO that process, transmit and store data; and
c) The Departmental networks that transport data.

The Information Security Policies are Department-wide policies that apply to all individuals who access, use or control Information Resources at the Department, including employees, as well as contractors, consultants and other agents of the Department and/or individuals authorized to access information resources by affiliated institutions and organizations.

This excludes all the transversal systems managed and controlled by State Information Technology Agency (SITA), Provincial Treasury and National Treasury.

Any authorisation of access to, or use of the network facilities provided by LDARD, shall be strictly subject to the provisions of this policy.

8. Definitions

Network Perimeter: The boundary between the private, locally managed-and-owned side of a network and the public and usually provider-managed side of a network.

Network Infrastructure: 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.

Firewall: A software or hardware-based network security system that controls the incoming and outgoing network traffic by analysing the data packets and determining whether they should be allowed through or not, based on a rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

Data: All items of information that are created, used, stored or transmitted by the LDARD community for the purpose of carrying out the departmental mission and used in the execution of the Department's required business functions.

9. Policy Pronouncements

9.1. Wired Network Connectivity

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

9.1.1. Network Access Point

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

a) The physical configuration
b) Connection points

c) The owner, or responsible official
d) The administrator
e) The purpose of the entry point
f) Software version and configuration

9.1.2. Network Perimeter Security

9.1.2.1. Approving Services

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

All proposed new entry points into the LDARD network, or proposed changes to existing entry points are approved by the Change Advisory Board.

9.1.2.2. Firewalls

9.1.2.2.1. Dedicated Functionality

All LDARD'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.

9.1.2.2.2. 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.

9.1.2.2.3. Intrusion Detection

All LDARD's firewalls must include Intrusion Detection Systems (IDS) approved by the Security Forum. These IDS must each be configured according to the specifications defined by the security standards.

9.1.2.2.4. External Connections

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

9.1.2.2.5. 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 Information Security Officer has been obtained, these privileges must be granted only to individuals who are full-time employees of LDARD.

9.1.2.2.6. 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 LDARD staff members.

9.2. GENERAL

9.2.1. DOCUMENTATION

Network operational procedures regarding all LDARDs' common network facilities shall be documented and safely stored.
The minimum documentation required is:

a) Roles and responsibilities of network staff
b) Network restore procedures
c) Network configuration settings for all critical equipment
d) Firewall configuration settings
e) Network diagrams clearly indicating logical connections and locations of the equipment on the network

All of the above points need to be reviewed on a regular basis as well as when a change in the network occurs.

9.2.2. CHANGE CONTROL

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

9.2.3. ACCESS

Access to network resources shall be managed through the LDARD User Account Management Policy.

9.2.4. INCIDENT MANAGEMENT

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

9.2.5. 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.

9.2.6. Malicious Software

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

9.2.7. Backup

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

9.2.8. 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.

9.3. ROLES AND RESPONSIBILITIES

Official	Responsibility	Alternate
Member of Executive (MEC)	Executive Authority of the policy	
Head of Department (HOD)	Accounting Officer of LDARD	
LDARD GITO	Ensure overall adherence to policy	LDARD IT Manager
LDARD Information Security Officer	Implement and ensure adherence to the policy	LDARD IT Manager
LDARD Network Administrators	Ensure all network related access comply with policy	
LDARD IT Users	Adhere to the provisions of this policy	

10. DEFAULT (Security Violation and Disciplinary Measures)

a) Security Violations

I) Any attempts to bypass security controls or to obtain unauthorized access or to make unauthorized use of a user account belonging to someone.
II) The use of LDARD's information assets for purpose other than for authorized business purposes.
III) The use of LDARD information assets for any unauthorized or illegal activity.
IV) Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure.
V) Any act (or failure to act) that results in sensitive or business critical information being disclosed to an unauthorized person.
VI) Any act (or failure to act) that results in sensitive or business critical information being modified or destroyed such that the LDARD or any of its branches / sub branches is adversely impacted.
VII) Any breach of this policy or any of its related.

b) Disciplinary Measures

Security violations will be considered as "misconduct" under the Department's Code of Conduct and may lead to disciplinary action under the Department's disciplinary procedure.

c) Reporting

All information abuses and security breaches should be reported to the Information Security Officer and GITO.

Non-compliance and deviations from this Policy is not acceptable. Should it be necessary to deviate from this Framework, the written permission and motivation from the HOD will be required.

11. INCEPTION DATE

The inception date for this policy will be its date of approval – as indicated on the cover page of this Policy document.

12. TERMINATION AND REVIEW CONDITIONS

This Policy will be reviewed every three years (3) or as and when a need arise. Should the Policy still be in the review process by the time it lapses, an extension period is applicable and the approved Policy remain valid until the reviewed version is approved.

13. ENQUIRIES AND REPORTING

Any enquiries with regard to any matter relating to this Policy or exemption requests shall be directed to the GITO Service Desk at the Limpopo Department of Agriculture and Rural Development, Tel. 015 294 3000.

GITO is responsible for the timeous review, circulation, advocacy, availability and feed-back regarding this Policy document. GITO is also responsible for reporting towards oversight bodies in the event of enquiries with regards to this Policy document.

Recommended by:

.....

Head of Department

(Maisela, RJ)

2017-09-12

.....

Date

Approved by:

.....

Hon MEC for Agriculture and Rural Development

Mapula Mokaba-Phukwana (MPL)

27/09/17

.....

Date