



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

Third Party Access Management Policy

Ref: 6/1/P

Date of effect: 13 June 2016

Recommended:

M. V. Schryver

Head of Department
(Maisela, RJ)

03/06/2016

Date

Approved:

M. Matshoge

MEC for Agriculture and Rural Development:
(Matshoge, BAJ)

13/06/16

Date

Table of contents	Page
1. Acronyms and abbreviations	1
2. Executive summary	2
3. Introduction	2
4. Purpose and objectives	2
5. Authority of the Policy	2
6. Legal Framework	2
7. Scope of application	3
8. Definitions	3
9. Policy Pronouncements	3
9.1 Principles	3
9.1.1 Risk Assessment	3
9.1.2 Third Party Access	4
9.1.3 General	5
9.1.4 Roles and responsibilities	6
10. Default	6
11. Inception date	7
12. Termination and review	7
13. Enquiries	7

1. Acronyms and abbreviations

GITO	Government Information Technology Office
HOD	Head of Department
IT	Information Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of the Executive Council
SITA	State Information Technology Agency

2. Executive summary

The Policy on the management of Third Party Access aims to address all relevant issues with regards to the management of third party access. It provides detailed information on the recording as well as agreements with regards to third party access and the roles and responsibilities are set out clearly. Restricted access is described fully and privileges are taken into consideration.

3. Introduction

Permitting access to third party can not only compromise the confidentiality of LDARD's information, but can also result in loss of data validity and integrity. LDARD shall control access to information processing facilities by third party organisations and access shall be assigned based on the assessment of the risk of granting such access. Permission of access and of any use of any information shall be governed through clauses built into third party agreements and contracts.

4. Purpose and objectives

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

The many variations in the profile of third parties, the technical and procedural mechanism for connecting them makes securing such connections a complex and challenging task. The objective of this policy is described as follows:

- a) To define the most secure method of providing third party access within LDARD.
- b) To ensure that only agreed and approved third parties gain access to the application.
- c) To ensure protection of key risk areas such as:
 - i) Unauthorised access to data.
 - ii) Theft of data.
 - iii) Confidentiality information becoming known to the public.

5. Authority

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

*SITA Act, of 1998

*Public Service Act, No 103 of 1994

REFERENCES:

- a) ISO 17799: Section 4.2
- b) CobIT: PO9, PO11
- c) ITIL Book: Service Level Management

7. Scope of application

This policy is applicable to third parties who may require access to LDARD's network. These include temporary staff; contactors; consultants; third parties; casuals; vendors and service providers. All third parties to whom access is granted are aware of the policy and act in accordance with it. Any authorisation of access to, or use of information resources provided by LDARD, shall be strictly subject to the provisions of this policy.

8. Definitions

Broadband	Refers to a telecommunications signal or device of greater bandwidth, in some sense, than another standard or usual signal or device (and the broader the band, the greater the capacity for traffic).
Dial-up	A form of Internet access that uses the facilities of the public switched telephone network to establish a dialled connection to an Internet service provider via telephone lines.
ISDN	Integrated Services Digital Network, a set of communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.

9. Policy pronouncements

Controls shall be put in place for third party access to LDARD's information resources. The following principles shall be adhered to, to comply with the policy:

9.1 Principles:

9.1.1 Risk Assessment

Business Need

Third-party access may put LDARD information at risk without adequate security management. Access will only be allowed if there is an appropriate business need. The type of connections and the strengths of the controls (e.g. monitoring and logging) for each type of connection shall be defined. The level of protection required shall be determined by risk assessment, approved by the application 'owner' and agreed by both parties in a documented text, such as a contract. The assessment shall consider:

- i) Types of access needed.

- ii) Value of the information.
- iii) Controls used by the third party.
- iv) Implications of access on the organisation's information security.

9.1.2 Third Party Access

A) Defining Third Party Access Connections

Third party connections and security considerations for each type of connection shall be clearly defined. Logging and monitoring of connections shall be done where appropriate.

B) Process for Third Party Access Connections

A process shall be implemented for authorising all third party connections to be LDARD's information systems which shall include:

- i) Access shall not be granted to third parties unless formal written agreement is signed with the respective third party.
- ii) Only authorised third parties shall be permitted access to IT resources to perform essential functions.

1) Restricted Access

Access to information resources by third parties shall be restricted to the minimum services and functions necessary for the business process. Third parties shall only have access to designated areas, as determined within the formal agreement, which is based on the business requirements. External access to applications shall be restricted by:

- a) Subjecting external users to strong authentication (e.g. challenge/response devices featuring one-time passwords, smartcards or other tokens).
- b) Routing traffic through firewalls.
- c) Limiting the methods of connection (e.g. broadband, ISDN or dial-up).
- d) Granting access only to specified parts of the application for maintenance and support.

Access shall only be increased if there is a business need and the appropriate risk analysis has taken place to reduce threats on the network.

2) Third Party Agreements

Third party users, and any subcontractor that is used by the third party, shall comply with all applicable information security policies, standards and procedures.

All Third Party agreements shall be formalised in a contract which shall contain at least the following:

- a) Timeframes for completion of transactions and arrangements for ensuring that transactions cannot be repudiated (e.g. by using 'digital signatures').
- b) Agreed security controls (e.g. access mechanisms, virus protection and back-up).
- c) Arrangements for managing changes and incidents.
- d) The right to audit security arrangements within the third party.
- e) Non-disclosure of information gained in the course of work.
- f) A requirement to return or destroy information or software at an agreed point.
- g) The respective liabilities of the parties to the agreement.
- h) Protection of intellectual property rights, copyright assignment and collaborative work.
- i) The right to monitor and revoke user activity.

These agreements shall be reviewed regularly to confirm that there is still a valid business requirement. Third party access shall not be allowed without such agreements being in place.

9.1.3 GENERAL

a) Review of Privileges

Authorisation for third party shall be revoked immediately when the third party service is no longer required or if a third party is deemed to be in breach of the third party agreement. Unused third party connections should be reviewed so as to ascertain the need for the connection on a regular basis.

b) Recording Third party Users

A record of all authorised third party users and their access rights shall be maintained and reviewed at least on a six (6) month basis. A register shall be kept by the Information Security Officer and shall contain:

- i) Duration and specific time periods.
- ii) When access is permitted.
- iii) A log of all access.

- iv) Authorised third party access users.
- v) Access levels provided.

The register shall be reviewed on a regular basis to confirm that there is still a valid business requirement of all third party accesses. As a technical security control IT Department shall set-up an expiry date on the Microsoft Active Directory (*User Identity and Access Management System*).

9.1.4 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 Deputy Director
Adherence to the policy	Third Party Users	No alternate

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 unauthorised access or to make unauthorised 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 authorised business purposes shall be considered a security violation.
- 3) The use of LDARD information assets for any unauthorised 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 unauthorised 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 LDARD 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

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

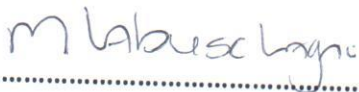
POLOKWANE

0700

Tel: 015 294 3000

E-mail: ITHelpDesk@agric.limpopo.gov.za

Recommended by:



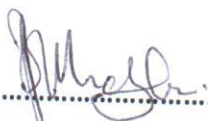
Maisela, RJ

(Head of Department)

03/06/2016

Date

Approved by:



Matshoge, BAJ

(MEC for Agriculture and Rural Development)

03/06/2016

Date