LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF AGRICULTURE

Third Party Access 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:

27/02/2012
Date

Comments:

_____

_____

_____

Table of Contents

1 ACRONYMS & DEFINITIONS

LDA	Limpopo Department of Agriculture
GITO	Government Information Technology Office
IT	Information Technology
SITA	State Information Technology Agency
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.

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 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:

- To define the most secure method of providing third party access within LDA.
- To ensure that only agreed and approved third parties gain access to the application.
- To ensure protection of key risk areas such as:

- Unauthorised access to data.
- Theft of data.
- Confidentiality information becoming known to the public.

5 SCOPE OF APPLICATION

This policy is applicable to third parties who may require access to LDA'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 LDA, shall be strictly subject to the provisions of this policy.

6 POLICY STATEMENTS

6.1 BACKGROUND

Permitting access tothird party can not only compromise the confidentiality of LDA's information, but can also result in loss of data validity and integrity. LDA 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.

6.2 PRINCIPLES

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

6.2.1 Risk Assessment

6.2.1.1 Business Need

Third-party access may put LDA 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:

- Types of access needed.
- Value of the information.
- Controls used by the third party.
- Implications of access on the organisation's information security.

6.2.2 Third Party Access

6.2.2.1 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.

6.2.2.2 Process for Third Party Access Connections

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

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

6.2.2.3 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:

- Subjecting external users to strong authentication (e.g. challenge/response devices featuring one-time passwords, smartcards or other tokens).
- Routing traffic through firewalls.
- Limiting the methods of connection (e.g. broadband, ISDN or dial-up).
- 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.

6.2.3 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:

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

6.3 GENERAL

6.3.1 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.

6.3.2 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:

- Duration and specific time periods.
- When access is permitted.
- A log of all access.

- Authorised third party access users.
- 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 Microsoft Active Directory (*User Identity and Access Management System*).

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
Adherence to the policy	Third Party Users	

6.5 SECURITY VIOLATION AND DISCIPLINARY MEASURES

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

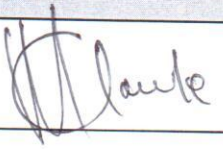
7 POLICY REVIEW

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 4.2
- CobIT: PO9, PO11
- ITIL Book: Service Level Management

9 ENDORSEMENT

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