LIMPOPO

PROVINCIAL GOVERNMENT

REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF AGRICULTURE

Data Backup 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

GITO	Government Information Technology Office
IT	Information Technology
LDA	Limpopo Department of Agriculture
SITA	State Information Technology Agency
Backup media	media you back up data on to, for example laptop, tape, CD-ROM, etc.
Information asset	Refers to electronic data, information, business application systems, operating systems, computer equipment and other IT infrastructure.
Server	is a physical computer dedicated to running one or more such service to serve the needs of users of the other computers on the 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 objective of this policy is to provide guidelines to ensure that data backup plans and procedures shall be in place to facilitate the normal functioning of critical LDA business activities in the event of failure or disaster.

5 SCOPE OF APPLICATION

This policy is applicable to all users including all temporary staff, contractors, service providers, or consultants who make use of LDA's information assets at LDA offices.

6 POLICY STATEMENTS

6.1 BACKGROUND

This policy serves to protect all information assets physically located at LDA, including all departments, where these systems are under jurisdiction and /or ownership of LDA. All users and staff who utilises such information assets are aware of the policy and act in accordance with it.

The policy set out the control conditions related to data backup activities within LDA. All types of data backup as may be required shall be made in accordance with the LDA data backup strategy.

6.2 PRINCIPLES

The following shall be adhered to, to comply with the policy requirements

6.2.1 Data Backup Strategy

A data backup strategy shall be developed and maintained and shall at the minimum include the following:

- Identification of critical data, information and software that needs to be backed up.
- The retention periods for backups of critical business process requirements.
- The frequency and type of information backup, based on the business process requirements.

Action taken in case of temporary or permanent loss; destruction or unavailability of information shall be clearly documented, forming a part of the LDA's standards and procedures.

6.2.2 Data Backed Up.

Data to be backed up include the following information:

- User data stored on the hard drive (My Document folder).
- System state data.
- The registry.

The following are systems to be backed up:

- File server.
- Mail server.
- Production web server (Internet).

- Applications servers.
- Domain controllers.
- Storage servers.
- Voice Infrastructure.
- Network Infrastructure.

6.2.3 Backup Cycles

The standard backup cycles as defines in LDA Data backup strategy is daily, weekly and monthly.

6.2.4 Data Retention

The **Electronic Communication and Transactions Act No. 25 of 2002** regulates electronic communication and prohibits the abuse of information. There are certain principles stated for the electronic collection of personal information and also the timeframe that this information must be kept:

	Document	Retention Period
9.1	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information.	As long asinformation isused, and atleast 1 yearthereafter.
9.2	A record of any third party to whom the information was disclosed.	As long asinformation isused, and atleast 1 yearthereafter.
9.3	All personal data which has become obsolete.	Destroy.

Data backups of systems shall be preserved indefinitely as long as the system is still in use by LDA.

6.2.5 Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

All critical systems shall have backup restore procedure.

6.2.6 Off-site Storage

Copies of backups will be stored in a safe location, physically distant from the data processing centre to facilitate disaster recovery efforts.

6.2.7 Testing

LDA IT Department is responsible for periodic testing of its backup and recovery services. System owners (example BAS, PERSAL etc.) and end users required to test and confirm successful recovery of information for which they are responsible.

6.2.8 Disposal

Backup media must be physically destroyed in a secure manner that renders the stored data irretrievable. Media destruction shall be conducted by authorized staff or by an approved designate.

6.2.9 Supporting Documentation

Documentation regarding the build and recovery of the implemented backup solution must be maintained in locations that allow for access during disaster recovery efforts. Tape and other backup media must be clearly labelled or barcoded to reflect the data written to the media and the date which the backup action occurred.

6.3 General

6.3.1 Data Backup Availability

Backup Information assets shall be readily available, but restricted to authorised individuals. In the event of a disaster, backup information assets are needed to implement disaster recovery. These shall be reliable and available at all times to the relevant authorised individuals within LDA.

6.3.2 Protection of Data Backups

In accordance with the LDA Physical and Environmental Security Policy, backups shall be protected from loss, damage and unauthorised access, by:

- storing them in a fireproof safe on-site , to enable important information to be restored quickly

- supporting them by copies kept off-site, to enable required systems to be restored using alternative facilities in case of a disaster
- restricting access to authorised staff

The level of protection afforded to off-site copies of backup information shall be the same as that of on-site backup material.

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 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 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 every year or as and when the need arise with the permissions from the MEC.

8 REFERENCES

- ISO 17799: Section 8.4.1
- CobIT: DS11.2, DS11.4
- ITIL Book: Release Management

9 ENDORSEMENT

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