



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA


DEPARTMENT OF AGRICULTURE

Information Classification 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	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.....	4
6.3	DESCRIPTION	5
6.4	CONFIGURATION	5
6.5	INFORMATION CLASSIFICATION	5
6.6	INFORMATION HANDLING REQUIREMENTS.....	6
7	ROLES AND RESPONSIBILITIES.....	8
8	REFERENCES.....	9
9	SECURITY VIOLATION AND DISCIPLINARY ACTIONS.....	9
10	POLICY REVIEW	9
11	ENDORSEMENT	10

1 ACRONYMS & DEFINITIONS

GITO:	Government Information Technology Office
IT:	Information Technology
LDA:	Limpopo Department of Agriculture
SITA:	State Information Technology Agency
Data Centre:	A facility used to house computer systems and associated components, such as telecommunications and storage systems.
Digital Signature:	A mathematical scheme for demonstrating the authenticity of a digital message or document.
Encryption:	The conversion of data into a form that cannot be easily understood by unauthorized people.
Information Asset:	Refers to electronic data, information, business application systems, operating systems, computer equipment and other IT infrastructure.
SSL:	Secure Session Layer, a protocol for encrypting information over the Internet.

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 ensure that all information assets are classified in accordance with business needs and the impacts associated with these needs. Its objective is to establish a common understanding and to provide guidelines and principles to apply classification levels in accordance with a classification scheme.

5 SCOPE OF APPLICATION

This policy applies to employees, contractors, consultants, temporaries, and other workers at LDA including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by LDA such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

6 POLICY STATEMENTS

This policy sets out the control conditions related to information classification activities within LDA.

6.1 BACKGROUND

LDA routinely gathers, stores, processes, transmits and disposes of records containing information. That information must be protected from unauthorised disclosure, misuse and misrepresentation while at the same time, made readily available to those who need it. Classification of information in terms of its business criticality is an essential element in achieving appropriate information security.

6.2 PRINCIPLES

All LDA information assets shall have a nominated owner, be classified, documented and verified.

The following principles shall be adhered to comply with the policy requirements:

6.2.1 Information Ownership

All critical information assets shall have a nominated owner. Owner for all critical information assets shall be identified. The owners or delegates shall be assigned the responsibility for the maintenance of appropriate controls over these information system assets. Responsibilities will be established at three levels as follows:

- **Data Owner**

Ownership is the management of an organisation unit, department, etc. where the information is created, or that is the primary user of the information. LDA retains actual legal ownership of information assets.

- **Custodian**

Custodians are employees designated by the Owner to be responsible for maintaining the safeguards established by the Owner.

- **User**

Users are employees authorised by the Owner to access information and use of the safeguards established by the Owner.

6.2.2 Inventory Register

Details of all critical information assets, as defined by LDA, shall be documented in an inventory register. The register shall include:

- Identification and Verification of Critical Systems.
- A formal process shall also exist to maintain critical information assets on the inventory. The process shall also cater for the inventory of critical information assets to be verified against the information system asset register on a regular basis.
- Every critical information system asset shall be uniquely identified. The identification mechanism used for this shall ensure that:
 - The location of the information assets is known.
 - The supplier, the purchase invoice number and the purchase invoice date of the information system asset is known.
 - Maintenance contract(s) for the information assets are identified and;
 - Person responsible for the information assets is known.

6.3 DESCRIPTION

A short description shall be available for every information system asset. The description shall include general information system assets, such as its main function and use.

6.4 CONFIGURATION

Technical configuration documentation shall be included and supported by business requirements explaining why the information system asset has been configured as such. This documentation shall include licensing information and version of hardware and software in use.

6.5 INFORMATION CLASSIFICATION

All information assets shall be classified based in their value and importance to LDA.

- **Top Secret**

Highly sensitive internal documents e.g. forensics reports, investment strategies, plans or designs that could seriously damage the LDA if lost or made public. Information in this category has very restrictive distribution and must be protected at all times. Security at this level is extremely high.

- **Confidential**

Information that is considered critical to LDA's on-going operations and could seriously impede the department if made public or shared internally e.g. employee salary details, medical certificate, etc... Such information should not be copied or removed from LDA's operational control without specific authority. Security at this level is high.

- **Internal Use Only**

Information not approved for general circulation outside LDA where its disclosure would inconvenience the organisation or management, but is unlikely to result in financial loss or serious damage to credibility. Examples include: internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.

- **Public Documents**

Information in the public domain, including annual reports, press statements, etc., security at this level is minimal.

6.6 INFORMATION HANDLING REQUIREMENTS

For each classification, several information handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of LDA information encompasses not only its confidentiality but also the need for integrity and availability.

The following table defines required safeguards for protecting data and data collections based on their classification.

Security Control Category	Data Classification		
	Public	Internal Use	Confidential/Top Secret
Access Controls	<p>No restriction for viewing.</p> <p>Authorization by Data Owner or designee required for modification; supervisor approval also required if not a self-service function.</p>	<p>Viewing and modification restricted to authorized individuals as needed for business-related roles.</p> <p>Data Owner or designee grants permission for access, plus approval from supervisor.</p> <p>Authentication and authorization required for access.</p>	<p>Viewing and modification restricted to authorized individuals as needed for business-related roles.</p> <p>Data Owner or designee grants permission for access, plus approval from supervisor.</p> <p>Authentication and authorization required for access.</p> <p>Confidentiality agreement required.</p>
Copying/Printing (applies to both paper and electronic forms)	<p>No restriction</p>	<p>Data should only be printed when there is a legitimate need.</p> <p>Copies must be limited to individuals with a need to know.</p> <p>Data should not be left unattended on a printer/fax.</p>	<p>Data should only be printed when there is a legitimate need.</p> <p>Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement.</p> <p>Data should not be left unattended on a printer/fax.</p> <p>Copies must be labelled "Confidential".</p> <p>Must be sent via Confidential envelope; data must be marked "Confidential".</p>
Physical Security	<p>System must be locked or logged out when unattended.</p>	<p>System must be locked or logged out when unattended.</p> <p>Hosted in a secure location required; A Secure Data Centre is recommended.</p>	<p>System must be locked or logged out when unattended.</p> <p>Hosted in a Secure Data Centre required.</p> <p>Physical access must be</p>

			monitored, logged, and limited to authorized individuals 24x7.
Data Storage	Storage on a secure server recommended. Storage in a secure Data Centre recommended.	Storage on a secure server recommended. Storage in a secure Data Centre recommended. Should not store on an individual's workstation or a mobile device (e.g., a laptop computer).	Storage on a secure server required. Storage in Secure Data Centre required. Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption. Encryption on backup media required. Paper/hard copy: do not leave unattended where others may see it; store in a secure location.
Transmission	No restrictions	No requirements	Encryption required (for example, via SSL or secure file transfer protocols). Cannot transmit via e-mail unless encrypted and secured with a digital signature.

7 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

8 REFERENCES

- ISO 17799: Section 5.1, 5.2
- CobIT: PO 2.3, PO2.4
- ITIL Book: IT Services Organisation

9 SECURITY VIOLATION AND DISCIPLINARY ACTIONS

- Any attempts to bypass security controls or to obtain unauthorized 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.

10 POLICY REVIEW

The policy shall be reviewed after every year or as and when the need arise with the permissions from the MEC.

11 ENDORSEMENT

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