



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA


DEPARTMENT OF AGRICULTURE

Information Security Policy

Ref: 6/1/P

Date of effect:

Recommended/ ~~Not Recommended~~

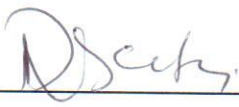


Head of Department

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	4
5	SCOPE OF APPLICATION.....	4
6	POLICY STATEMENTS	4
6.1	BACKGROUND.....	4
6.2	POLICY STATEMENTS	4
6.2.1	Information access	4
6.2.2	Access by Third parties	5
6.2.3	Non-repudiation	5
6.2.4	Information Asset Classification and Control	5
6.2.5	Physical and environmental security.....	5
6.2.6	Virus protection.....	6
6.2.7	Compliance with Copyright Regulations	6
6.2.8	Security monitoring	6
6.2.9	Personnel Security.....	6
6.2.10	Disaster Recovery Planning (DRP)	6
6.2.11	Exchanges of information.....	6
6.3	CUSTODIAN OF THE POLICY.....	7
6.3.1	The Information Security Officer is responsible for:	7
6.3.2	Internal Audit unit	7
6.3.3	Users.....	7
6.3.4	IT Department	7
6.3.5	GITO.....	8
6.4	SECURITY VIOLATION AND DISCIPLINARY MEASURES	8
7	POLICY REVIEW	9
8	ENDORSEMENT	9
	ANNEXURE A: ACCESS TO INFORMATION ASSETS FORM.....	9

1 ACRONYMS & DEFINITIONS

LDA	Limpopo Department of Agriculture
GITO	Government Information Technology Office
IT	Information Technology
SITA	State Information Technology Agency
Information asset:	Refers to electronic data, information, business application systems, operating systems, computer equipment and other IT infrastructure.
Information processing facility:	A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.
Non-repudiation:	The ability to prove that a person participated in all or part of an interaction
Repudiation:	Denial by a person involved in an interaction, e.g. communication, processing, transaction, of having participated in all or part of the interaction.
Security incident:	Any event that has, or could have, resulted in loss or damage to company assets, or an action that is in breach of company security procedures.
Third parties:	Any company or individual providing services to or receiving services from LDA requiring access to information or IT infrastructure.
User:	User is any employee, contractor or third-party Agent of LDA who is authorized to access LDA information asset.

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

- a) To protect information from unauthorized disclosure or intelligible interception;
- b) Safeguard the accuracy and completeness of information;
- c) To ensure that information and IT services are available when required;
- d) To protect information and information technology from misuse;

5 SCOPE OF APPLICATION

The scope of this policy is applicable to:

- a. All LDA employees, contractors and consultants and includes users affiliated to third parties who are authorized to access electronic information owned by LDA.
- b. The IT infrastructure required to create, process, transmit, share or store sensitive or business critical information.

6 POLICY STATEMENTS

6.1 BACKGROUND

Information is a critical resource required for the achievement of business objective. Information and information technology resources are subject to accidental, criminal, malicious and natural threats that could potentially cause financial loss, disruption to business continuity, loss of goodwill and commercial image.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures, technological solutions and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

6.2 POLICY STATEMENTS

6.2.1 Information access

- Information security access controls shall be in place to ensure that all users are uniquely identified and authenticated.
- Information security access controls shall be in place to ensure that users are only able to access the information assets for which they have been properly authorized.

- Information security access controls shall be in place to ensure that users are only able to access information assets with authorized privileges and access levels.
- Access to information assets shall only be granted to individuals having a legitimate, authorized business need.
- There must be a formal user registration and de-registration procedure for granting access to all LDA IT systems.
- A formal process must be conducted at regular intervals to review user's access rights.
- All users must follow good security practices in the selection and use of passwords.

6.2.2 Access by Third parties

- The risk associated with access to information asset by third parties must be assessed and appropriate security controls implemented.
- Access to information asset by third parties shall be monitored.
- All third party users shall sign an undertaking that the information security policy has been read, understood and complied with.

6.2.3 Non-repudiation

- Information security audit control shall be in place to ensure accountability for and non-repudiation of system actions.
- A user having authorized access shall be accountable for the actions associated with the user account assigned to them.

6.2.4 Information Asset Classification and Control

- An inventory of information assets shall be drawn up and maintained.
- Information assets shall have a nominated owner who shall be responsible for ensuring that the assets are appropriately controlled.
- Classification and associated protective controls for information must be suited to business needs for sharing or restricting information and business impact associated with such needs.

6.2.5 Physical and environmental security

- Access control measures shall be implemented to ensure that only authorized personnel are allowed access to information processing facilities.
- Appropriate protective measures shall be implemented to protect information assets from loss, damage, or disruption caused by natural disasters or equipment failure.

- Equipment must be maintained in accordance with manufacturer's instructions and/or documented procedure to ensure its continued availability and integrity.
- Information must be erased from equipment prior to disposal or re-use.
- No employee must be allowed to remove property from LDA premises.

6.2.6 Virus protection

- Measures to detect prevent and eliminate viruses and other malicious or destructive programs shall be implemented and kept current.
- All security updates must be applied to all systems.

6.2.7 Compliance with Copyright Regulations

- Any program or software protected by copyright shall only be copied in accordance with license agreements or with the owner's consent.

6.2.8 Security monitoring

- All security violations shall be recorded, reported, reviewed and addressed.

6.2.9 Personnel Security

- Appropriate personnel security measures shall be taken to reduce the risk of human error, theft, fraud or misuse of facilities.
- Appropriate awareness and educational programmes shall be carried out to ensure that personnel are aware of their responsibilities and the risks to information assets.
- Information security policies and procedures must be readily available to all employees.

6.2.10 Disaster Recovery Planning (DRP)

- Disaster recovery plans and procedures shall be documented, implemented, tested and maintained to ensure the continuation of operations should computer processing or data communications be interrupted for any reason for a defined unacceptable period of time.

6.2.11 Exchanges of information

- E-mail must only be provided to LDA employees or long term contractors.
- No offensive material must be sent using e-mail.

- Content scanning must only be enforced in checking for malicious software, viruses or violations.
- Functional policy for use of email must be developed and controls must be put in place to reduce security risks created by electronic mail.
- Authorised users must be provided with Internet access for business use.
- Sites deemed unsuitable for business use will be blocked.

6.3 CUSTODIAN OF THE POLICY

6.3.1 The Information Security Officer is responsible for:

- Developing security policies, standards and procedures;
- Information security strategy planning and implementation;
- Information security awareness and education;
- On-going evaluation of the effectiveness of security measures;
- Security event monitoring and response;
- The implementing physical and technological security measures;
- Virus protection;
- Disaster Recovery planning;
- Provision and management of facilities for security audit trails and event logs.

6.3.2 Internal Audit unit

- Responsible for auditing compliance with this policy and for investigations into security violations.

6.3.3 Users

- Adhering to policies, guidelines and procedures pertaining to the protection of LDA information asset.
- Reporting actual or suspected vulnerabilities in the confidentiality, integrity or availability of LDA information asset to Helpdesk, or the Information Security Office.
- Reporting actual or suspected breaches in the confidentiality, integrity or availability of LDA information asset to Helpdesk or Information Security Office.

6.3.4 IT Department

- Understanding and reporting on how data is stored, processed and transmitted.

- Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of LDA information asset.
- Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of LDA information asset.
- Provisioning and de-provisioning of user access.
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of LDA information asset.

6.3.5 GITO

- Overseeing the review and approval of Information Security Policy

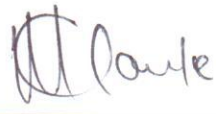

6.4 SECURITY VIOLATION AND DISCIPLINARY MEASURES

- 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 Manager.

7 POLICY REVIEW

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

8 ENDORSEMENT

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

ANNEXURE A: ACCESS TO INFORMATION ASSETS FORM

This form is to be used, when authorizing access to LDA information assets. Eventually, the form must be submitted to GITO.

ACCESS TO INFORMATION ASSETS OF THE LDA

File:

Tel. No.:

Enquiries:

The Head of Department
Department of Agriculture
Private Bag X9487
Polokwane
0700

Attention: Government Information Technology Officer

I,.....,identity number.....,
PERSAL number, hereby:

Classification	Description	Reason	Access date
Hardware (Laptop/PC/printer)			
Standard (Email, Internet, standard packages)			
Internal application/systems (Business specific)			
Transversal systems			
Network access (for guest user)			

1. I have read the all Information Technology Policies;
2. I understand its terms and conditions;
3. I have initialed every page of the Policy;
4. I hereby submit a copy of the Policy with initialed pages to the HR Personnel Office for safe-keeping and custody;
5. I undertake to abide by the stipulations and provisions of the Policies during the period of my employment; and that
6. In the event of my violation of the policy prescripts, I will subject myself to the discipline that the Head of Department that may exercise against me in terms of laws, regulations, agreements and delegations of authority governing my employment.

Name:

Signature:

Date: