



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

Information and Communication Technology
Security Policy

REF: 6/1/P

Version 1.0 – 2017

Date of approval: 2 Jan 2018

Recommended by:


.....

Head of Department
(Maisela RJ)

2017-12-19
.....

Date

Approved by:


.....

Hon Member of Executive Council (Acting)
Sekoati, SC (MPL)

2018/01/2
.....

Date

Table of Contents	Page
1. Acronyms and abbreviations	1
2. Executive Summary	2
3. Introduction	2
4. Purpose and objectives of the Policy	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 Authorised use	4
9.2 Acceptable use	4
9.3 Security awareness	4
9.4 Continuity plan	5
9.5 Monitoring and reporting	5
9.6 Risk assessment	5
9.7 Asset management	5
9.8 Breach of Policy and sanctions	5
9.9 Development of specific ICT policies, procedures and guidelines	6
9.10 Incident reporting	6
9.11 Incident management	6
10. Default	7
11. Inception date	7
12. Termination and review	7
13. Enquiries and Reporting	8

1 ACRONYMS AND ABBREVIATIONS

CGICT	Corporate Governance for ICT
DPSA	Department of Public Service and Administration
GICT	Governance for ICT
GITO	Government Information Technology Office
GITS	Government Information Technology Services
HOD	Head of Department
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
ISG	Information Security Group
ISO	International Standards Organisation
IT	Information Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Council
MISS	Minimum Information Security Standards
SITA	State Information Technology Agency

2 EXECUTIVE SUMMARY

This Policy addresses all matters regarding Information and Communication Technology security in the Limpopo Department of Agriculture and Rural Development (LDARD). The Policy refers to risk assessment as well as asset management, incident reporting and incident management. It also addresses the matter of security awareness and indicate authorised use and acceptable use. The Information and Communication Technology (ICT) Continuity Plan is discussed and attention is given to the implementation and monitoring of this Policy.

3 INTRODUCTION

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

ICT Security management is the implementation of a suitable set of controls which include, but are not limited, to policies, practices, procedures, standards, guidelines, organisational structures, technological solutions and software functions. These controls need to be established to ensure that the specific security objectives of an organisation are met.

This Policy is aligned to the Department of Public Service Administration (DPSA) ICT Security Guideline issued in May 2017.

4 PURPOSE AND OBJECTIVES

This Policy specifies the principles and requirements the Limpopo Department of Agriculture and Rural Development (LDARD) has established to protect information assets owned by or in the care of the Department.

The Policy also fulfils the requirements of the Department for Public Service and Administration (DPSA) Corporate Governance of Information and Communication Technology (CGICT).

5 AUTHORITY OF THE POLICY

This Policy is issued under the authority of both the Member of Executive Council (MEC) for LDARD as the Executive Authority of the LDARD, and the Head of Department (HOD) as the Accounting Officer of LDARD.

6 LEGAL FRAMEWORK

- a) King III Code Chapter 5 – King III Governance of Information Technology
- b) ICT House of Values
- c) COBIT 5 – A business framework for the governance and management of enterprise IT from ISACA
- d) DPSA Corporate Governance for ICT (CGICT)

- e) ISO 27001 - Information Security Management Systems Standard by the International Standards Organisation
- f) MISS – Minimum Information Security Standards

7 SCOPE OF APPLICATION

The information resources included in the scope of the ICT Security Policy are:

- a) All Data (as defined below) stored on Department's owned ICT;
- b) Departmental computing hardware and software systems supported by Government Information Technology Office (GITO) that process, transmit and store Data; and
- c) Departmental Networks that transport Data.

The ICT Security Policy is a Department-wide policy that apply to all individuals who have access, use or control information resources in the Department, including employees, as well as contractors, consultants and other agents of the Department and/or individuals authorized to access information resources by affiliated institutions and organisations.

This excludes all the transversal systems managed and controlled by State Information Technology Agency (SITA), Provincial Treasury and National Treasury as well as (GIS).

8 DEFINITIONS

Government Information Technology Officer (GITO): Director that is ultimately accountable for security policies and for ensuring that appropriate security controls and mechanisms are in existence and enforced throughout the organisation.

Government Information Technology Services (GITS): Departmental Directorate responsible for the management of information technology.

Information asset: A definable piece of information stored in any manner, deemed valuable to the organisation. This includes information as well as information systems and infrastructure throughout the organisation that support the storage, distribution, processing, access and control of information.

Information Security Group (ISG): The central governance entity in charge of key information security functions such as developing information security policies, responding to information security incidents and measuring compliance with policies.

Data: All items of information that are created, used, stored or transmitted by the LDARD community for the purpose of carrying out the departmental mission and used in the execution of the Department's required business functions.

Department: Refer to the LDARD.

ISO: Refer to Information Security Management Systems Standard by the International Standards Organisation.

9 POLICY PRONOUNCEMENTS

The Information Security Policy is based on the principles set out in the International Standards Organisation (ISO) for Information Security (ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management) to deliver the Department’s mission of the Information Security Management Programme which is to protect the confidentiality, integrity and availability of data. In line with that mission the Department has developed this ICT Security Policy to:

- a) Protect information assets handled by ICT;
- b) Act as a responsible conservator of information assets entrusted to its care;
- c) Provide direction and support for ICT security in accordance with business requirements, regulations, legal requirements and contractual obligations;
- d) State the responsibilities of staff, partners, contractors and any other individual or organisation having access to the Department’s ICT systems;
- e) State management intent to support the goals and principles of security in line with business strategy and objectives;
- f) Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained;
- g) Optimise the management of risks by preventing and minimising the impact of ICT security incidents;
- h) Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required;
- i) Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats;
- j) Ensure ICT Security requirements are regularly communicated to all relevant parties; and
- k) Ensure business processes shall be consistent with the above principles, and, unless contrary to law, and government regulations, shall follow the Department’s ICT Security Management Standards and procedures for implementation of those standards.

9.1 AUTHORISED USE

Access to ICT systems and information for which the Department is responsible is permitted in support of the Department’s areas of business or in connection with a service utilised by the Department. Authorised users are defined as: Department employees, consultants, authorised contractors, temporary staff, partner organisations or members of the public when using public information services provided by the Department.

9.2 ACCEPTABLE USE

All users of ICT systems and information for which the Department is responsible must agree to and abide by the terms of the Department’s Acceptable Use Policy, associated security policies and applicable Codes of Conduct.

9.3 SECURITY AWARENESS

The Department is committed to promoting safe working practices. All employees will receive security awareness training commensurate with the classification of information and systems to which they have access to. Staff working in specialised roles will receive appropriate training relevant to their roles. Relevant ICT Security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of ICT Security policies and procedures.

9.4 ICT CONTINUITY PLAN

The Department has developed and maintains an ICT Continuity Plan. The plan is based on specific risk assessment to maintain critical business functions in the event of any significant disruption to services or facilities on which the Department is reliant.

9.5 MONITORING AND REPORTING

The Department reserves the right to monitor the use of ICT systems and information, including email and internet usage to protect the confidentiality, integrity and availability of the Department's information assets and ensure compliance with the Department's policies. The Department may, at its discretion, or where required by law, report security incidents to the relevant authorities for further investigation. As part of the standard audit review process, Internal Audit will routinely assess compliance with the Department's ICT Security Policy and applicable ISO27001 controls and report matters to senior management where appropriate. Security incidents reported through the Security Incident Management Policy and Procedures will inform on the effectiveness of controls and assist in identifying training and awareness requirements and improvements.

9.6 RISK ASSESSMENT

The Department has developed a Risk Management Strategy and the risk to the Department's ICT systems and information will be managed under this framework, with reference to the guidelines detailed in *ISO/IEC 27005:2010 Information security management systems – Part 3: Guidelines for information security risk management*. Reviews are independent, unbiased and verified by either Internal Audit or external parties when required.

9.7 ASSET MANAGEMENT

The Department will maintain an inventory consisting of all information assets which will be managed in accordance with the Department's ICT Security policy and procedures.

9.8 BREACH OF POLICY AND SANCTIONS

Breach of this Policy and/or security incidents can be defined as events which could have, or have resulted in loss or damage to the Department's assets, or an event which is in breach of the Department's security procedures and policies as defined in the ISMS Charter section 9 (Default (Security Violation and Disciplinary Measures)).

All Departmental employees, consultants, contractors and vendors have a responsibility to report security incidents and breaches of this Policy as quickly as possible through the Department's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Department.

GITO, in cooperation with Executive Management, other Sub-branch management and administrators will enforce this Policy, and establish standards, procedures, and protocols in support of the Policy.

The Department will take appropriate measures to remedy any breach of the Policy and its associated standards, procedures and guidelines through the relevant frameworks in place. In the case of an individual the matter may be dealt with under the disciplinary process.

Failure of the Department's employees to comply with the Department's ICT Security Policy is "misconduct" under the department's code of conduct and may lead to disciplinary action under the Department's disciplinary procedure.

Failure of contractors, temporary staff, public, partners or third party organisations to comply with the Department's ICT Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

Violations of law may also be referred for criminal or civil prosecution. Additionally, violations of this Policy may result in termination or suspension of access, in whole or in part, to the Department's information systems at the discretion of the GITO, where such action is reasonable to protect the Department or the Department's information infrastructure.

9.9 DEVELOPMENT OF SPECIFIC ICT POLICIES, PROCEDURES AND GUIDELINES

The Department is committed to the ongoing development and review of ICT policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. A list of current supporting documents is included in <http://e-docs/ITServices/IT%20Policies/Forms/AllItems.aspx>. New policies, procedures and guidelines are distributed to all stakeholders at the time of issue.

9.10 INCIDENT REPORTING

Users will be continually made aware of and encouraged to use a page on the Department's Service Desk Management System where they can report any breaches online or via a telephone call to the IT Service Desk. Breaches can involve not only information technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern or which may contravene the Department's Code of Conduct and associated policies.

9.11 INCIDENT MANAGEMENT

During reporting of a breach, details of the incident will be entered into the call logging system - either by the person directly reporting the incident using the form on the Service Desk system or by the Service Desk agent taking the call. Once the call has been entered into the system, an email is generated and sent to the ICT Security Officer and also copied to the GITO Director. The ICT Security Officer will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representative to deal with. Representatives looking into security breaches will be responsible for updating, amending and modifying the status and clearance code of incidents in the call logging system.

10 DEFAULT

The Policy will be applicable at all times. Breach of this Policy will be considered as an offence.

a) Security Violations

- I) Any attempts to bypass security controls or to obtain unauthorized access or to make unauthorized use of a user account belonging to someone.
- II) The use of LDARD's information assets for purpose other than for authorized business purposes.
- III) The use of LDARD information assets for any unauthorized or illegal activity.
- IV) Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure.
- V) Any act (or failure to act) that results in sensitive or business critical information being disclosed to an unauthorized person.
- VI) 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.
- VII) Any breach of this policy or any of its related.

b) Disciplinary Measures

Security violations will be considered as "misconduct" under the Department's Code of Conduct and may lead to disciplinary action under the Department's disciplinary procedure.

c) Reporting

All information abuses and security breaches should be reported to the Information Security Officer and GITO.

Non-compliance and deviations from this policy is not acceptable. Any request for deviation to this policy need to be made in writing and approved by the Accounting Officer.

11 INCEPTION DATE

The inception date for this Policy will be its date of approval.

12 TERMINATION AND REVIEW


This Policy will be reviewed every three years (3) or as and when a need arise. Should the Policy still be in the review process by the time it lapses, an extension period is applicable and the approved Policy remain valid until the reviewed version is approved.

13 ENQUIRIES AND REPORTING

Any enquiries with regard to any matter relating to this Policy or exemption requests shall be directed to the GITO Service Desk at the LDARD, Tel. 015 294 3071.

GITO is responsible for the timeous review, circulation, advocacy, availability and feed-back regarding this Policy document. GITO is also responsible for reporting towards oversight bodies in the event of enquiries with regards to this Policy document.

Recommended:


.....

Head of Department
(Maisela, RJ)

2017-12-19
.....
Date

Approved:


.....

Hon Member of Executive Council (Acting)
Sekoati, SC (MPL)

2018-01-2
.....
Date