LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

Information and Communication Technology Risk Management Policy

Ref: 6/1/P

Reviewed Version 1.0; 2017

Date of approval: 27 September 2017

Recommended by:

.... 2017-09-13

Head of Department **Date**

(Maisela, RJ)

Approved by:

.... 27/9/2017

Hon MEC for Agriculture and Rural Development **Date**

(Mokaba-Phukwana, M)

Table of Contents

1. ACRONYMS AND ABBREVIATIONS

DPSA	Department of Public Service Administration
GITO	Government Information Technology Office
HOD	Head of Department
ICT	Information and Communication Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Council
SITA	State Information Technology Agency

2. Executive summary

This Policy is addressing all matters regarding Information Security Risk Management within the Limpopo Department of Agriculture and Rural Development. Apart from the definitions, Scope of application, default and matters such as the legal framework within which this Policy has been developed, it also address matters such as risk remediation, risk monitoring and risk analyses.

3. Introduction

As the business has adopted information technology to aid it in the execution of the business tasks, there are risks brought in by this technology and thus measures have to be put in place to limit the impact of these risks. Information Technology (IT) controls result from an effective risk assessment process. Therefore, the ability to mitigate IT risks is dependent upon risk assessments. Senior management should identify, measure, control, and monitor technology to avoid risks that threaten the safety and soundness of an institution.

The department has adopted a risk based approach to the management of its information security management. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations.

The following activities related to managing organizational risk will be used to manage the information security program and will be applied to both new and legacy information systems within the context of the system development life cycle and the organizational enterprise information technology architecture:

a) **Categorize -** Categorize the information system and the information resident within that system based on impact.

b) **Select** - Select an initial set of security controls for the information system based on the security categorization and the minimum security requirements defined; apply tailoring guidance as appropriate; and supplement the tailored baseline security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyzes, or special circumstances.

c) **Implement -** Implement the security controls in the information system.

d) **Assess -** Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

e) **Authorize -** Authorize information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.

f) **Monitor -** Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analysis of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

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

4. Purpose and objectives

As provided in the Limpopo Department of Agriculture and Rural Development (LDARD) Information Security Charter (the "Charter"), the Department is charged with protecting the confidentiality, integrity and availability of its Information Resources (as defined in the Charter). To accomplish this task, a formal Information Security Risk Management Program has been established as a component of the Department's Information Security Program (as defined in the Charter) to ensure that the Department is operating with an acceptable level of risk. The Information Security Risk Management Program is described in this Policy.

5. Authority of the policy

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

6. Legal framework

a) SITA Act, of 1998
b) Public Service Act, No 103 of 1994

7. Related policies, standards & procedures:

a) Information Security Charter
b) Desktop and Server Configuration Standards
c) Network Security Policy
d) Information Security Risk Management Standard
e) Information Security Risk Management Procedure
<u>Departmental Policies:</u>
Limpopo Department of Agriculture and Rural Development Risk Management Policy

8. Scope of application

The information resources (the "Information Resources") included in the scope of the Information Security Policies are:

b) All data (as defined in Section 8 below) regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);

c) The Departmental computing hardware and software Systems Supported by GITO that process, transmit and store data; and

d) The Departmental Networks that transport data.

The Information Security Policies are Department-wide policies that apply to all individuals who access, use or control Information Resources at 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 organizations.

This excludes all the transversal systems managed and controlled by SITA, Provincial Treasury and National Treasury.

9. Definitions

Information Asset: Information of value which is owned and/or used by an organization.

Vulnerability: A weakness in the asset that can be exploited.

Threat: An agent or an event that can exploit the vulnerability.

Impact: The consequence (damage) if the threat exploits the vulnerability.

Probability of occurrence: The possible number of times the threat can exploit the vulnerability in a given time period.

Risk: The potential of loss (an undesirable outcome, however not necessarily so) resulting from a given action, activity and/or inaction.

IT Risk: Any risk related to information technology. It is the final impact expressed as a mathematical term that combines:

a. The value of the asset
b. The probability of occurrence (threat exploiting the vulnerability)
c. The impact of the threat exploiting the vulnerability

Risk = Threat × Vulnerability × Asset Value

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.

10. Policy Pronouncements

Information Security Risk Management covers all of the Department's Information Resources, whether managed or hosted internally or externally. Management, System Owners, Data Owners and IT Custodians are responsible for working with the Information Security Office to implement the Information Security Risk Management Program, including remediation of identified risks in a timely manner.

The Information Security Risk Management Program is comprised of the following processes:

10.1 Information Resource Risk Categorization

All Information Resources that store, process or transmit data are included in the Information Security Risk Management Program. Information Resources are categorized based on their function, threat exposure, vulnerabilities and data type pursuant to the Information Security Policies. The categorization process takes into account the following elements:

a) Size, complexity and capabilities of the Information Resources and organizations;

b) Technical infrastructure, hardware and software capabilities;

c) Cost of implementing security controls; and

d) Probability and criticality of risks to data, particularly sensitive data or confidential data.

Resources to address risks are allocated according to the identified risks.

10.2 Security Control Selection

The appropriate security controls to mitigate identified risks are selected based on the nature, feasibility and cost effectiveness of the controls. The Department has selected elements from the following security control frameworks to use as part of its Information Security Risk Management Program:

a) International Standardisation Organisation 27002, Security Techniques – Code of Practice for Information Security Management;

b) ITIL- Industry Standard Framework for IT Service Management Guidelines and Best Practices;

c) NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations.

d) COBIT 5

All systems and endpoints must meet the baseline requirements as defined in the Desktop and Server Configuration Standards or the Network Security Policy. Additional controls will be evaluated based on the framework defined above and applied based on risk analysis.

10.3 Risk Analysis

A documented risk analysis process is used as the basis for the identification, definition and prioritization of risks. The risk analysis process includes the following:

a) Identification and prioritization of the threats to Information Resources;

b) Identification and prioritization of the vulnerabilities of Information Resources;

c) Identification of a threat that may exploit a vulnerability;

d) Qualitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific vulnerability; and

e) Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources.

The risk analysis process is updated when environmental, operational or technical changes arise that impact the confidentiality, integrity or availability of Information Resources. Such changes include:

a) New threats or risks with respect to the Information Resources;

b) An information security incident;

c) Changes to information security requirements or responsibilities. (e.g., new laws or regulations, new role defined in the institution, new or modified security controls implemented, etc.); and

d) Changes to the Department's organizational or technical infrastructure that impacts Information Resources (e.g., addition of a new network, new hardware/software standard implemented, new method of creating, receiving, maintaining or transmitting data, etc.).

When security measures for an Information Resource do not meet a security standard, risks are identified and expressed. Three factors are considered when determining the risk:

a) Type of possible threat and its likelihood;

b) Extent of effectiveness of current security controls or their vulnerability; and

c) Likely level of impact.

Risks are qualitatively expressed as Critical, High, Medium, Low and Minimal. For the purposes of this Policy, Critical, High, Medium, Low and Minimal Risks are defined as follows:

a) Critical Risk: The risk of imminent compromise or loss of sensitive data from either external or internal sources or where sensitive data has already been exposed. There is no control in place to protect the data.

b) High Risk: The risk of imminent compromise or loss of sensitive data from either external or internal sources. There is only a single control, or multiple ineffective controls, in place to protect the data.

c) Medium Risk: The risk of compromise or loss of sensitive data is possible from either external or internal sources, although less likely from external sources. Controls are in places that are somewhat effective to protect the data.

d) Low Risk: The risk of compromise or loss of sensitive data is possible, but not probable or an Information Resource might be used to obtain access to sensitive data on a different Information Resource.

e) Minimal Risk: There is no realistic risk of compromise or loss of sensitive data.

10.4 Risk Remediation

The strategies for risk remediation are proportionate to the risks to the Information Resource. The selected and implemented risk management measures reasonably protect the confidentiality, integrity and availability of Information Resources and the risk is managed on a continuous basis. One or more of the following methods are used to manage risk:

a) Risk elimination, mitigation or reduction;
b) Risk avoidance;
c) Risk acceptance; and/or
d) Risk transference

A Low or Minimal Risk may be accepted by the GITO with appropriate documentation and periodic reviews. If a previously accepted risk is realized in a real incident, the risk analysis and management are repeated with the new information, and re-addressed with greater sensitivity and urgency based on the nature and extent of the incident.

10.5 Risk Monitoring

The results of Risk Analysis and Risk Remediation are documented and reviewed by Management, the Information Security Office, System Owners, Data Owners and IT Custodians. The Monitoring processes are used to evaluate:

a) The effectiveness of security controls;

b) Changes to Information Resources and environments of operations; and

c) Compliance with laws and regulations, industry standards and Department policies.

The frequency of risk monitoring will be based on:

a) Regulatory compliance requirements;

b) The importance or sensitivity of the Information Resource;

c) The requirements of the Information Security Policies; and

d) The degree to which Systems are interconnected to one another and the risk posed by such connections.

11. Default

a) 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)).

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

Non-compliance and deviations from this Policy is not acceptable. Should it be necessary to deviate from this Framework, the written permission and motivation from the HOD will be required.

12. Inception Date

The inception date for this policy will be its date of approval – as indicated on the cover page of this Policy document.

13. Termination and Review Conditions

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.

14. Enquiries and reporting

All enquiries regarding this policy should be directed to:

Information Technology Service Desk, Limpopo Department of Agriculture and Rural Development, Polokwane.

Tel: 015 2943000

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 by:

.... 2017-09-13 ....

Head of Department **Date**

(Maisela, RJ)

Approved by:

.... 27/09/17 ....

Hon MEC for Agriculture and Rural Development **Date**

Mapula Mokaba-Phukwana (MPL)