LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

ICT Change Management Policy

Ref: 6/1/P

Date of effect: ..15..December...2016

Recommended:

_____ 2016/12/13

Head of Department Date

(Maisela, RJ)

Approved:

_____ 15/12/16

Hon MEC for Agriculture and Rural Development: Date

Mapula Mokaba-Phukwana (MPL)

Table of Contents

1. Acronyms and abbreviations:

CAB	Change Advisory Board
CI	Compliance Inspection
ECAB	Emergency Change Advisory Board
COBIT	Control Objectives for Information and related Technology
FSC	Forward Schedule Change
GITO	Government Information Technology Office(r)
ICT	Information Communication Technology
IEC	International Electro-technical Commission
ISO	International Organisation Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
KPI	Key Performance Indicator
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Council
OLA	Operational Level Agreement
RFC	Request for Change
SIP	Service Improvement Plan
SITA	State Information Technology Agency
SLA	Service Level Agreement
SLR	Service Level Requirement
UC	Underpinning Contract
URL	Uniform/Universal Resource Locator

2. Executive summary

The ICT Change Management Policy aims to coordinate, control and manage all ICT changes in the Department. This policy sets out how changes should be addressed and managed to benefit the organization and minimize risk and potential impact to the business.

The roles and responsibilities is set out clearly and the objectives of the policy is described in detail.

3. Introduction

The purpose of this policy is to set the rules which will apply to all changes and the people involved in analysing or assessing, building, testing or implementing changes. The ultimate goal of the policy is to ensure minimum disruption to the overall business activities of LDARD and its entities.

The Change Management Process shall be governed by the following guiding principles:

a) Manage information in respect of any modification, addition or deletion of a component in the IT infrastructure, systems and documentation which could potentially impact on LDARD to deliver a quality service.
b) This implies that all changes will be logged and tracked in ITSM tool or solution at the Service Desk and the Configuration Management Database shall be updated as described in the Change Management process and sub-processes.

4. Purpose and objectives

The following are key objectives of this policy:

i. To ensure that the Change Management process is adhered to and in line with ITIL.
ii. To standardize Change Management processes throughout LDARD GITO.
iii. To ensure that LDARD GITO provides a world class service to LDARD customers and its entities, by maintaining their infrastructure up to the expected norms and standards.
iv. To ensure that there is minimum downtime experienced for LDARD customers and entities.
v. To ensure that all possible risks are considered when approving changes.
vi. To ensure that LDARD IT infrastructure that is in scope of LDARD GITO is protected from unauthorized and undocumented changes which may be in breach of legal or governance requirements.
vii. To enable effective governance over the Change Management Process.
viii. To ensure that the Configuration Management Database's integrity is preserved.

5. Authority

This policy is issued under the custodianship of the Accounting Officer and the Honourable MEC for Agriculture and Rural Development in Limpopo.

6. Legal Framework

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

References

- ISO 17799: Section 8.1.3
- COBIT 5
- ITIL Book: Incident Management

7. Scope of application

This policy applies to all permanent and temporary staff within LDARD as well as contractors and visitors who work and/or visit LDARD. This policy also applies in respect of 3rd party suppliers and LDARD customers/clients and their respective personnel, who use services provided by LDARD in respect of the communications channel available and the procedures to be followed to bring issues to the attention of, or to submit requests to LDARD. As such, these policy guidelines shall be referenced in Service Level Agreements and/or contracts and applicable sections provided to customers.

8. Definitions

For the purpose of this policy, the following definitions of terminology will be applicable:

Change:	Means service changes as well as infrastructure and operational changes.
Severe:	Impact that can lead to a complete loss of service or could potentially pose a threat to the integrity of the whole of LDARD
Critical:	Changes that require immediate action and if not implemented immediately, will leave the Department open to huge risk/s (financially and other). All Severe impact changes will have a Critical urgency
Major:	Change that affects a lot user (more than 50%)

9. Policy Pronouncements

All Change Requests must adhere to the LDARD GITO Change Management Policy and must therefore follow the process as outlined in the Change Management Process document. Service and infrastructure changes must have a clearly defined and documented scope, desired outcome and back-out plan.

a) Line Managers are responsible for ensuring that the relevant staff members are suitably trained to support this policy.
b) All Change Management documentation shall be maintained on the LDARD GITO portal or file server which will be communicated by LDARD IT.
c) This policy and all supporting documentation must be communicated and made available to all relevant stakeholders either by formal distribution or by placement on an accessible portal.

9.1 Directive

All changes shall be recorded in ITSM tool or solution and initiated, controlled and implemented within the documented Change Management Process.
There will be no exception to this directive, unless duly authorized by GITO, as complete and comprehensive records form the basis of strategic decisions.
Major and emergency changes shall be classified and managed according to the Change Management Process and with due consideration in accordance with the CAB process.
This policy shall be brought to the attention of all new and existing staff and other relevant stakeholders by means of Policy advocacy conducted by IT.

9.2 Dependencies

For the successful implementation of this policy, the following is required:

a) Executive Management.
b) Commitment and acceptance to change by all staff.
c) Adherence to Change Management Process and Procedure.
d) Competence, awareness and training of all supporting staff fulfilling responsibilities of the Change Management Process owner.
e) Adherence to all ITIL® practices with specific emphasis on Change Management Process.

9.3 Change Management Process

The role of the Change Management Process is to ensure that new services and changes to services are assessed, approved, implemented and reviewed in a controlled manner with minimum risk to the business.

9.3.1 Change records must be analysed regularly to detect increasing levels of changes, frequently recurring types, emerging trends and other relevant information.

9.3.2 The results and conclusions drawn from change analysis shall be recorded.

9.3.3 Actions for improvement identified from Change Management shall be recorded and input made into a Service Improvement Plan (SIP) for improving the service.

9.4 Change Initiation

9.4.1 All operational changes (i.e. changes to the live environment) need to be requested at least seven working days prior to implementation.

9.4.2 All changes must be a triggered by a properly filled out RFC form (see annexure A), and managed through the documented Change Management Process.

9.4.2.1 RFC form must be completed in full and reviewed for completeness by the assigned Change Coordinator.

9.4.3 All Changes must be logged in ITSM tool or solution with the RFC form attached.

9.5 Change Classification

All changes need to be classified according to how much impact they will have on the business and service provision. Below are some clear definitions of types of changes. These changes will all have different priorities based on assessed urgency and impact levels depicted further below:

Type of Change	Description / Definition
Minor Changes	• These usually entail the correction of one or more specific errors and are often modifications that implement documented emergency solutions correctly. Normally contain small enhancements and fixes, some of which may already have been issued as emergency fixes. Usually associated with an impact classification of "Minor". • If not deemed to have an Enterprise wide impact, these changes must be considered by the Change Management Process Owner, Change Coordinator and other identified stakeholders.

Standard Changes	• Standard Changes are well known, low risk and their implementation steps are proven and documented. As such they don't need formal Change Management approval for each occurrence. • Change Management approval is however needed to classify a certain type of Change as a Standard Change. Standard Changes have their own process and procedure which is simpler than a normal Change. • The list of Standard Changes can be found on LDARD GITO portal or file server which will be communicated by LDARD IT.
Urgent Changes **(Emergency)**	• Urgent changes must be approved by the Emergency Change Advisory Board. • Urgent changes are only permitted where/when the implementation of the Change is to resolve or prevent an event, or to address identified security vulnerabilities with a classified impact of "Severe" and a classified urgency of "Critical". • The possibility exists that all Priority "0" changes would be deemed Urgent, but care must be taken to ensure that changes do not get classified as such to simply fast-track implementation, since testing is optional (if sufficient time is not available) for Urgent changes and documentation may be done ex post facto. • Every Emergency Change must follow the full Change Management process, except for the testing phase which may be skipped ONLY if there is no time and if it is approved by the ECAB.
Major Changes	• Represent a significant change of hardware and software and which introduce important modifications to functionality, technical characteristics, etc. Normally contain large areas of new functionality, some of which may eliminate temporary fixes to problems. Usually associated with an impact classification of "Severe", "Major" and "Significant". • Major changes must be considered by the local CAB.

9.6 Change Prioritization

Change prioritization will be based on two criteria:

a) Potential impact associated with the services and SLA(s) effected (Impact)
b) Speed with which the change needs to be effected (Urgency)

Change prioritization is the sequence in which changes need to be rolled-out or implemented, based on impact and urgency as defined below. The rationale for this approach is that although the impact (previously: severity) associated with a particular change might be high; the urgency to have it implemented might be low, thus enabling LDARD GITO to strategically commit resources and capabilities.

Although it is likely that a high-impact change will also be urgent, this is not always the case. A change may have a high impact on a customer, but low urgency if the customer does not require a solution to be implemented for six months. Alternatively, a change could have a high urgency but low impact.

9.6.1 Priority

Priority must be associated with the services and SLA's affected or potentially affected. Service level agreements formalize the relationship between LDARD GITO and the customer base. Changes must be linked with the correct SLA to allow correct classification according to potential impact of the services/customers associated with the SLA. This quickly and accurately establishes the change's urgency and its impact on the business, as the SLA identifies the service/s affected, the users of that service, and the consequences of service interruption. It also records the expected timescales for return to normal and, if specified, the arrangements for the invocation of business continuity planning.

The tables that follows provides the default association of Impact and Urgency from which Priority is derived.

9.6.2 Impact

This signifies business impact and efficiency. The impact of a change must be determined by the effect it has on the business of the LDARD. The determination of impact in this way can only be effectively undertaken in agreement with the affected stakeholder during the development of the SLA. Factors that must be considered are:

a) The number of customers/users affected (or could potentially be affected).
b) The extent to which business degradation results (or could potentially result).
c) The stage in the business cycle when the change is implemented.

Impact	Definition
0 - Severe	Any change where the impact could lead to a complete loss of service or could potentially pose a threat to the integrity of the whole of LDARD.
1 - Major	A change where the potential impact to service could lead to: 1) A loss of more than 50% of total capacity; or 2) A loss of more than 50% of served targets (origins/destinations) not reachable;
2 - Significant	A change where the potential impact to service could lead to: 1) A loss of less than 50% of total capacity; or 2) A loss of all redundancy (exposure to complete service outage); or 3) A loss of a served target (origin/destination not reachable); or 4) Material (financially – penalties) impact to LDARD - GITO;
3 - Minor	A change where the potential impact could: 1) Degrade the quality of service; or 2) Affect a small number of individuals or CI's—for example, a change to a printer used by a department (risk is less because of LDARD experience level in respect of the proposed change); this has to be noted in the SLA.
4 - Inconsequential	Any change that doesn't have any potential to impact directly on service delivery in respect of existing services to existing customers, such as: 1) Request for a new service; or 2) Amendment of supporting documentation; or

Impact	Definition
	3) A change with a set release mechanism (standard change)

9.6.3 Urgency

This signifies the urgency of the request. This relates to the speed with which a change needs to be implemented according to its impact.

Urgency	Definition
0 - Critical	Immediate action required. Changes, if not implemented immediately, will leave the LDARD open to huge risk (financially and other).
1 - High	A change that must be implemented immediately, but doesn't have a Severe Impact.
2 – Medium	A change that must be implemented as soon as possible – associated with partial denial of service with an impact on a large number of customers.
3 - Low	A change that must be implemented as soon as possible – associated with partial denial of service on a limited number of customers or degradation in the quality of service.
4 - Scheduled	A change that is not required to be implemented as classified above or a request for a new service.

9.7 Remedial Planning

The Change Management Process should include the manner in which the change is to be reversed or remedied if unsuccessful.

i. Previous configuration information is kept until the effected changes are tested and confirmed to be functional.

9.8 Change Approval

All changes shall be approved by the Change Management Process Owner, assisted by the Change Advisory Board where necessary. The Change Management Process Owner may decide which additional people to invite in order to assist the CAB in assessing the change, depending on the nature of the change to be made.

9.9 Change Authorization Mandate

Prior to the approval of ICT changes, clear indication on the nature of change shall be provided to enable the correct workflow associated with the required approval.

Changes will be approved as follows:

Urgent/Emergency	GITO and/or CAB to approve
All other changes	Approved by the CAB

9.10 Change Review

All changes must be reviewed after implementation and the results of this review must be documented in ITSM tool or solution. This review must cover the following:

a) Whether the change met its objectives.
b) Whether the change stayed within its budget.
c) Whether the implementation went as planned.
d) Whether the change has an impact on the customer's business operations.

9.11 Change Freeze Periods

Change Freeze Periods are imposed in order to protect the IT infrastructure, application and/or other business activities from any change activity that may undermine its stability and operation.

The change freeze is imposed during Financial Year End and upon requests from other institutions (e.g. Treasury).

The change Freeze periods depend largely on what information is available from the business, ideally there would be a calendar of business events well ahead of schedule where times could be identified as well as dates when change freezes are required. In this way everyone knows well in advance that making of changes is not possible at that time and can therefore plan around those dates in advance.

9.12 Urgent/Emergency Change (Exemption/deviation)

All Urgent / Emergency changes must be referred to the Change Management Process Owner for evaluation and authorisation. The Change Management Process Owner can be contacted on Tel: +27 15 294 3058 or e-Mail: ITHelpDesk@agric.limpopo.gov.za

The GITO has the sole right to exempt a person or application from this policy, or part thereof. The exemption will be null and void unless:

a) It is in writing
b) It is signed and dated by GITO
c) A record is kept of the exemption

9.13 Roles and Responsibility

Issue	Person Responsible	Alternate
Has overall responsibility for adherence to policy	LDARD GITO	LDARD IT Manager
Has the responsibility for implementation and adherence to the policy	LDARD ISO	

10. Default

No deviation from this policy is allowed. Should any deviation be needed, it will only be granted with the written approval of the Accounting Officer – after thorough investigation and motivation.

a) 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.
b) The use of LDARD's information assets for purpose other than for authorised business purposes shall be considered a security violation.
c) The use of LDARD information assets for any unauthorised or illegal activity shall be considered a security violation.
d) Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure shall be considered a security violation.
e) 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.
f) 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 shall be considered a security violation.
g) Any breach of this policy or any of its related documents shall be considered a security

violation.

h) Any person charged with a security violation shall face disciplinary action.
i) All information abuses and security breaches should be reported to the Information Security Officer.

11. Inception date

The date of approval (as indicated on the cover page of this policy) is also the date of inception.

12. Termination and Review

This policy should be reviewed every 24 months (2 years) or as and when a need arise.

13. Enquiries

All enquiries regarding this policy should be directed towards:

The Director: IT

Limpopo Department of Agriculture and Rural Development

PO Box 9487

POLOKWANE

0700

Tel: 015 294 3000

E-mail: ITHelpDesk@agric.limpopo.gov.za

Recommended by:

..... 20/6/12/13

Maisela, RJ **Date**

(Head of Department)

Approved by:

..... 15/12/16

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

Mapula Mokaba-Phukwana (MPL)

Annex A: Request For Change Form

Request For IT Change Form (RFC)

Name:

Job Title:

Date:

Business Function:

Telephone:

Cell No:

E-Mail:

Request For Change Number:

Date Service Required:

Related RFC / Incident No:

Priority Level: Urgent

☐ High TICK

☐ Medium

☐ Low

Description of Change:

Business Reason:

Effect of NOT implementing Change:

Platforms Affected:

☐ E-Mail ☐☐ SMS ☐ NT – OS Changes X☐ ☐NT – Domains ☐ LAN ☐☐ WAN ☐ Intranet X Internet

☐☐ Firewall ☐☐ Antivirus ☐☐ Transversal Systems ☐ ☐Websites ☐ Desktop hardware/software ☐☐ Other

Impact to Users:

☐ All Users Affected

☐ >100 Users Affected

☐ <100 and >10 Users Affected

X <=10 Users Affected

Back out / Recovery Plan?

Has Change Been Implemented (In case of an Emergency Change)? ☐ Yes ☐ No

If Yes, who approved the Emergency Change?

Impact Assessment :

Capabilities of Change Implementer:

Request For IT Change Form (RFC)

Training Requirements (Includes Change Implementer and Helpdesk):

_____

Cost of Implementing Change (Includes Third Party/Resource Cost):

Name Change Owner:

Work Stream

Signatures:

Requested By : Change Owner: _____ Date: ____/____/____

Approved By : Departmental Line Manager: _____ Date: ____/____/____

Ratified By : Work Stream Director _____ Date: ____/____/____

Change Manager Approval

Approved By: _____ Date: ____/____/____

Planned Implementation Date: ____/____/____

Completed Implementation Date: ____/____/____

Completed By: _____ Date: ____/____/____

Implementation Results: _____

_____

_____

_____

_____

Approved By GITO: _____ Date: ____/____/____