



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
SPORT, ARTS AND CULTURE

| | |
|-------------------------|---|
| Name of Department | Department of Sport, Arts and Culture |
| Name of the policy | ICT data backup policy |
| Date of Approval | 31/3/2023 |
| Date of Review | 31/3/2026 |
| Version | |
| Responsible Directorate | Communications and Information Technology (Government Information Technology Office) |
| Reference Number | 4/5/P |
| Unique number | 4/5/P-4 |

Table of contents

| Contents | Page |
|---|------|
| 1. Acronyms and abbreviations | 3 |
| 2. Executive summary | 4 |
| 3. Introduction | 4 |
| 4. Purpose and objectives of the policy | 4 |
| 5. Authority of the policy | 4 |
| 6. Legal Framework | 4 |
| 7. Scope of application | 5 |
| 8. Definitions | 5 |
| 9. Policy pronouncements | 5 |
| 9.1 Data Back-up Strategy | 5 |
| 9.1.1 Data Classification | 6 |
| 9.1.2 Back-up Cycles | 6 |
| 9.1.3 Data Retention | 6 |
| 9.1.4 Restoration | 6 |
| 9.1.5 Testing | 6 |
| 9.1.6 Disposal | 7 |
| 9.1.7 Supporting documentation | 7 |
| 9.1.8 Data back-up availability | 7 |
| 9.1.9 Storage and protection of data back-ups | 7 |
| 9.2 Roles and Responsibilities | 7 |
| 10. Default | 8 |
| 11. Inception date | 8 |
| 12. Termination and review conditions | 8 |
| 13. Enquiries and Reporting | 8 |
| 14. Policy approval | 9 |

1. Acronyms and abbreviations

| | |
|--------------|---|
| | Disaster Recovery Site |
| GITO | Government Information Technology Office |
| ICT | Information Communication and Technology |
| IT | Information Technology |
| LDARD | Limpopo Department of Agriculture |
| SITA | State Information Technology Agency |
| COBIT | Control Objectives for Information and related Technology |
| ISO | International Organization for Standardization |
| MEC | Member of Executive Council |
| LDSAC | Limpopo Department of Sport Arts and Culture |
| DSS | Deliver, Service and Support |

2. Executive summary

The Data back-up Plan addresses all matters relevant to the backing-up of data. It endeavours to ensure that no information is lost without the possibility of recovering it. The strategy, classification, cycles as well as testing, restoration, recovery and availability is discussed in detail.

3. Introduction

All electronic information must be copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

This policy serves to protect all information assets physically located at LDSAC, including all sub-branches, where these systems are under the jurisdiction and /or ownership of LDSAC. All users and staff who utilise such information assets are aware of the policy and act in accordance with it.

The policy sets out the control conditions related to data backup activities within LDSAC. All types of data backup as may be required shall be made in accordance with the LDSAC Data Backup Strategy.

4. Purpose and objectives of the policy

The purpose of this policy is to provide for the continuity, restoration and recovery of critical data and systems as well as ensure critical data are backed up periodically and copies maintained at an off-site location.

The objective of this policy is to provide guidelines to ensure that data backup plans and procedures shall be in place to facilitate the normal functioning of critical LDARDRD business activities in the event of failure or disaster.

5. Authority of the policy

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

- SITA Act
- Public Service Act
- Electronic Communication and Transactions Act

References include:

- 1) ISO 17799: Section 8.4.1
- 2) CobIT: DS11.2, DS11.4
- 3) ITIL Book: Release Management

7. Scope of application

This policy, except otherwise indicated, is applicable to all ICT infrastructure, processes and systems managed by GITO. The policy also applies to all LDSAC employees, temporary staff, contractors, service providers, or consultants who make use of LDSAC's information assets at LDSAC offices.

Data custodians (GITO) are responsible for providing adequate backups to ensure the recovery of electronic information in the event of failure. These backup provisions will allow LDSAC business processes to be resumed in a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple generations of backups should be maintained.

The long-term retention of information (e.g., financial records) will be met using separate archive policy and procedures, as determined by Records Management

8. Definitions

| | |
|--------------------------|--|
| Backup media | media you back up data on to, for example laptop, tape, CD-ROM, etc. |
| Information asset | Refers to electronic data, information, business application systems, operating systems, computer equipment and other IT infrastructure. |
| Back-up | The process of copying active files from online disk to device so that files may be restored to a disk in the event of equipment failure, damage to or loss of data. |
| Archive | The process of moving inactive files from online disk to a tape, i.e. deleting the files from copying them, in order to release online storage for reuse. |
| Restore | The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server. |
| Server | is a physical computer dedicated to running one or more such service to serve the needs of users of the other computers on the network |

9. Plan pronouncements

9.1 DATA BACKUP STRATEGY

The following shall be adhered to, to comply with the plan requirements:

The data backup strategy includes the following:

- Identification of critical data, information and software that needs to be backed up.
- The retention periods for backups of critical business information requirements.
- The frequency and type of information backup, based on the business process requirements.

Action taken in case of temporary or permanent loss; destruction or unavailability of information shall be clearly documented, forming a part of the LDSAC's standards and procedures.

9.1.1 Data Classification

Data to be backed up include the following information:

- User data on My Documents and desktop folder excluding multimedia files
- System state data.
- System Application.

The following core infrastructure and systems are to be regularly backed up:

- I. Mail server.
- II. Production web server (Internet and external website).
- III. Applications and database servers.
- IV. Domain controllers.
- V. Storage servers.

9.1.2 Backup Cycles

The standard backup cycles shall be daily, weekly, monthly and annual.

9.1.3 Data Retention

The **Electronic Communication and Transactions Act** regulate electronic communication and prohibit the abuse of information.

In line with the requirements the Electronic Communication and Transactions Act all personal information "must, for as long as the personal information is used and for a period of at least one year thereafter".

Backups of systems and data shall be preserved as follows:

- For Directors to MEC for three years.
- For all other users and systems for one year.

9.1.4 Restoration

Requests for file restoration must be made through the GITO help desk. The request should include information about the name of the file, if known, the last time it was changed, and the date and time it was deleted or destroyed.

All critical systems refer to Disaster recovery Strategy for the Application.

9.1.5 Testing

LDSAC GITO is responsible for periodic testing of its backup and recovery services at least every three months. System owners (i.e. BAS, PERSAL etc.) and end users

are required to check and confirm successful recovery of information for which they are responsible.

9.1.6 Disposal

Backup media must be physically destroyed in a secure manner that renders the stored data irretrievable. Media destruction shall be conducted by Records Management.

9.1.7 Supporting Documentation

Documentation regarding the build and recovery of the implemented backup solution must be maintained in locations that allow for access during disaster recovery efforts. Tape and other backup media must be clearly labelled or barcoded to reflect the data written to the media and the date which the backup action occurred.

9.1.8 Data Backup Availability

Backup Information assets shall be readily available, but restricted to authorised individuals. In the event of a disaster, backup information assets are needed to implement disaster recovery. These shall be reliable and available at all times to the relevant authorised individuals within LDARDRD.

9.1.9 Storage and Protection of Data Backups

Copies of backups will be replicated to the Disaster Recovery Site every day to facilitate recovery efforts in the event of a disaster.

In accordance with the LDSAC Physical and Environmental Security Policy, backups shall be protected from loss, damage and unauthorised access, by:

- a) Storage in a safe on-site location, to enable important information to be restored quickly
- b) Supporting them by copies kept at the DR Site, to enable required systems to be restored using alternative facilities in case of a disaster
- c) Restricted access to authorised staff

The level of protection afforded to off-site backup copies shall be the same as that of on-site backup material.

9.2 ROLES AND RESPONSIBILITIES

| Official | Responsibility |
|-----------------------------------|-----------------------------------|
| Member of Executive Council (MEC) | Executive Authority of the policy |
| Head of Department (HOD) | Accounting Officer of LDLSAC |

| | |
|------------------------|---|
| LDSAC GITO | To ensure adherence to policy |
| LDSAC ISO | To ensure implementation and adherence to the policy |
| LDSAC IT Users | Adhere to the provisions of this policy |
| System Administrators | Ensure their systems and related data is backed up according to this policy |
| Network Administrators | Ensure all network infrastructure configuration is backed up according to this policy |

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.

1. 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.
2. The use of LDSAC's information assets for purpose other than authorised business purposes shall be considered a security violation.
3. The use of LDSAC information assets for any unauthorised or illegal activity shall be considered a security violation.
4. Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure shall be considered a security violation.
5. 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.
6. Any act (or failure to act) that results in sensitive or business critical information being modified or destroyed such that the LDSAC or any of its branches / sub branches is adversely impacted shall be considered a security violation.
7. Any breach of this policy or any of its related documents shall be considered a security violation.
8. Any person charged with a security violation shall face disciplinary action.
9. 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 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 remains valid until the reviewed version is approved.

13. Enquiries and Reporting

All enquiries regarding this policy should be directed towards:

The Deputy Director: GITO

Limpopo Department of Sport Arts and Culture

PO Box 9549, POLOKWANE, 0700.

Tel: 015 284 4136

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.

14. Policy approval


Recommended / ~~Not Recommended~~



HEAD OF DEPARTMENT

31/03/2023
DATE

Approved / Not Approved



MEMBER OF EXECUTIVE COUNCIL

31/03/2023
DATE