dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

INFORMATION COMMUNICATION TECHNOLOGY BACKUP AND RETENTION POLICY

ICTBRP VERSION 1.1

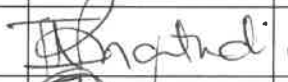
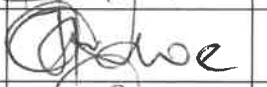
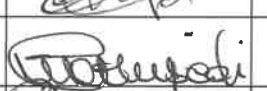
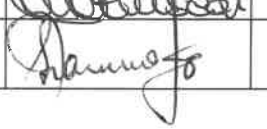
Document Details

Author	Directorate Information Communication Technology
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Information Communication Technology Backup and Retention Policy
Sensitivity	Internal Use Only
Effective Date	After the Accounting Officer's signature
Created Date	29-10-2018
Version Date	<date of Accounting Officer's signature>

Change Record

Modified Date	Author	Version	Description of Changes
01-10-2022	Directorate ICT	1.0	Alignment to the current environment

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer & Director Information Communication Technology		12/10/22
Ms K. Phatudi	ICT Governance Champion		12/10/22
Ms F. Nchoe	Chairperson: ICT Steering Committee		12/10/22
Ms M. Dayel	Chairperson: ICT Strategic Committee		12/10/22
Ms M.G. Mothibedi	Departmental Chief Risk Officer		12/10/22
Mr P. Namate	Director Legal Services		12/10/22

Records Management Sign–Off

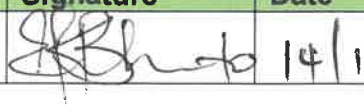
Name	Position	Signature	Date
Mr E. Khuto	Acting Deputy Director Records Management		14/10/2022

TABLE OF CONTENTS

1. Introduction 1
2. Regulatory and Guidance Framework 1
3. Objective of the policy 2
4. Aim of the policy 2
5. Scope of Application 2
6. Data Backup Standards 2
7. Data Backup Selection 3
8. Types of Backup 3
9. Backup Schedule 5
10. Data Backup Procedures 6
11. Storage Medium 6
12. Data Backup Owner 7
13. Off-site Storage 7
14. Retention Considerations 8
15. Recovery of Backup Data 8
16. The role of Backups in Records Management 9
17. Verification of Backups 9
18. Policy Compliance 10
19. Review 10
20. Approval 10

Glossary of Terms

Backup	refers to making copies of data so that the copies may be used to restore the original data after a data loss event
Battle box	A container - often literally a box or brief case - in which data and information are stored so as to be immediately available post incident.
DCS&TM	Department of Community Safety and Transport Management
Department	Department of Community Safety and Transport Management
DITO	Department Information Technology Officer
Electronic media	Means electronic storage media which may include Internet, CD-ROMs, DVD, HDD and any other medium that requires electricity or digital encoding of information.
HoD	Head of Department
Information Communication Technology (ICT)	The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
Data Retention	is the continued storage of departmental data for compliance or business reasons.
User	Employee accessing the system for the purpose of processing or authorising transaction, updating or amending system data or extracting Management reports from such system.
Stakeholders	refers to any of the following: Provincial Internal Audit (PIA), Auditor General of South Africa (AGSA), State Information Technology Agency (SITA), Office of the Premier (OTP) and Provincial Government Information Technology Officer (PGITO)

1. Introduction

The Department shall ensure that the departmental data is stored in an on-site and off-site location and can be easily accessible in the event of an equipment failure or disaster. Lack of productivity and cost of reproducing data can seriously harm the department.

2. Regulatory and Guidance Framework

The following legislation was considered when drafting this policy:

i. Constitution of the Republic of South Africa Act, Act No. 108 of 1996
ii. Copyright Act, Act No. 98 of 1978
iii. Electronic Communications and Transactions Act, Act No. 25 of 2002
iv. Minimum Information Security Standards, as approved by Cabinet in 1996
v. National Archives and Record Service of South Africa Act, Act No. 43 of 1996
vi. National Archives Regulations and Guidance
vii. Promotion of Access to Information Act, Act No. 2 of 2000
viii. Promotion of Administrative Justice Act, Act No. 3 of 2000
ix. Protection of Personal Information Act, Act No. 4 of 2013
x. Regulation of Interception of Communications Act, Act No. 70 of 2002
xi. Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

3. Objective of the policy

This policy seeks to outline the process of continuity, restoration and recovery of critical data. The System Administrator needs to ensure that critical data is backed up and stored in an offsite location.

4. Aim of the policy

The aim of this policy is to ensure that the Departmental ICT Systems conform to a standard backup and recovery control process and seeks to define the controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.

5. Scope of Application

This policy applies to all employees in the Department as well as other stakeholders utilising the departmental ICT systems. This policy is crucial for the effective protection of departmental data. All users have the responsibility to ensure compliance to this policy document.

6. Data Backup Standards

6.1 Critical data, which is critical to the system, must be defined by the system administrator and must be backed up.

6.2 Backup data must be stored at a location that is physically different from its original creation and usage location, along with a "battle box".

6.3 Data restores must be tested monthly.

6.4 Procedures for backing up critical data and the testing of the procedures must be documented. These procedures must include, as a minimum, for each type of data:

(a) Definition of a specific data to be backed up;
(b) The type(s) of backup to be used (e.g. full backup, incremental backup, etc.);
(c) The frequency and time of data backup;

(d) The number of generations of backed up data that are to be maintained (both on site and off site);

(e) Responsibility for data backup;

(f) The storage site(s) for the backups;

(g) The storage media to be used;

(h) Any requirements concerning the data backup archives;

(i) Transport modes; and

(j) Recovery of backed up data.

7. Data Backup Selection

- All data and software essential to the continued operation of Departmental systems must be backed up.
- All supporting material required to process the information must be backed up, this includes programs; control files, install files, and operating system software.
- The application owner, together with the DITO, will determine what information must be backed up, in what form, and how often.

8. Types of Backup

8.1 Full backups should be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site.

8.2 Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.

8.3 In the event that a system requires a high degree of skill to recover data from backup, consider taking full images of the servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.

Type	Detail	Frequency
Full Data Backup	Is a method of backup where all the files and folders selected for the backup will be backed up. It is commonly used as an initial or first backup	Weekly and Monthly
Incremental Data Backup	This procedure stores the files which have been changed since the last incremental / full backup. Incremental data backups are always based on full data backups and must be combined periodically with full data backups. For example, if a full backup was performed on Monday, Tuesday's incremental will back up all changed files since Monday's backup. However, Wednesday's incremental will only back up files that have changed since Tuesday's incremental backup and so on until another full backup is performed.	Daily
Differential Data Backup	Is a type of backup that copies all the data that has changed since the last full backup. For example, if a full backup is done on Sunday, Monday's differential backup backs up all the files changed or added since Sunday's full backup.	Daily
Image Backup	Is a backup process for a computer or virtual machine (VM) that creates a copy of the operating system (OS) and all the data associated with it, including the system state and application configurations. The backup is saved as a single file that is called an image.	Daily

9. Backup Schedule

Choosing the correct Backup Schedule:

- Backup schedules must not interfere with day to day operations. This includes any end of day operations on the systems.
- A longer backup window might be required, depending on the type of backups chosen.

Frequency and time of data backup:

- When the data in a system changes frequently, backups needs to be taken more frequently to ensure that data can be recovered in the event of a system failure.
- Immediate full data backups are recommended when data is changed to a large extent or the entire database needs to be made available at a certain point in time.

9.1 Previous versions

- The previous two versions of operating systems and applications must be retained at the off-site storage location;
- Annual, monthly and weekly backups must be retained at the off-site location.

10. Data Backup Procedures

The DITO must choose between automated and manual backup procedures based on their requirements and constraints. Both procedures are in line with best practice. The table below outlines the two procedures with their advantages and disadvantages.

Type	Detail	Advantages	Disadvantages
Manual Backup	Manual triggering of the backup procedures.	The operator can individually select the interval of data backup based on the work schedule.	The effectiveness of the data backup is dependent on the discipline and motivation of the operator.
Automatic Backups	Triggered by a program at certain intervals	The backup schedule is not dependent on the discipline and reliability of an operator	There is a cost associated with automation. The schedule needs to be monitored and revised to include any non-standard updates and/or changes to the work schedule.

11. Storage Medium

When choosing the data media format for backups, it is important to consider the following:

(a) Time constraints around identifying the data and making the data available;

(b) The storage capacity;

(c) The cost of data backup procedures and tools vs. cost if restored without backup;

(d) The importance of data;

(e) Reliability of data media;

(f) Retention schedules; and

(g) Confidentiality and integrity.

12. Data Backup Owner

The Programme Manager must delegate two employees (One primary, one secondary) to commit and adhere to each backup schedule.

13. Off-site Storage

- Data backups must be stored in two locations:

  (a) One on-site with current data in machine-readable format in the event that operating data is lost, damaged or corrupted; and

  (b) One off-site to additionally provide protection against loss to the primary site and on-site data.

- Off-site backups must be a minimum of 6 kilometres from the on-site storage area in order to prevent a single destructive event from destroying all copies of the data.

- Should high availability be required, additional backup copies should be stored in the immediate vicinity of the ICT system.

- Minimum requirements are to store the weekly, monthly and or yearly backup sets off site.

- Weekly and monthly backups must be stored offsite for the entire duration of the retention period.

- Receipts of media being collected and delivered must be kept for record keeping purposes and must be signed by ICT staff in attendance.

- Should an off-site media be required to perform a restore, the data media must be returned to the offsite facility for the remainder of the retention period
- All data media used to store confidential information must be disposed of in a manner that ensures the data is not recoverable.

14. Retention Considerations

A possible retention schedule is as follows:

(a) A full system backup will be performed weekly. Weekly backups will be saved for a full month.

(b) The last full backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled by the backup system.

(c) Monthly backups will be saved for one year, at which time the media will be reused.

(d) Yearly backups will be retained for five years and will only be run once a year at a predetermined date and time.

(e) Differential or Incremental backups will be performed daily. Daily backups will be retained for two weeks. Daily backup media will be reused once this period ends.

15. Recovery of Backup Data

1. Backup documentation must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:

   (a) Identification of critical data and programs; and

   (b) Documentation and support items necessary to perform essential tasks during a recovery process.

2. Documentation of the restoration process must include:

(a) Procedures for the recovery.

(b) Provision for password (access) management if the data is encrypted (protected).

3. Recovery procedures must be tested monthly.

4. Recovery tests must be documented and reviewed by the ICT System Administrator.

16. The role of Backups in Records Management

1. The ICT Manager must work with the Records Manager to ensure that data in electronic form are managed, protected and retained for as long as they are required.
2. The role of backups in records management is more suited as a means to recover electronic records management systems in the event of a disaster or technology failure.
3. The DITO is responsible for the following, when backing up electronic records:

(a) Backups must be made daily, weekly and monthly;

(b) Backups must cover all data, metadata, audit trail data, operating systems and application software;

(c) Backups must be stored in a secure off-site environment;

(d) Backup files of public records must contain the subject classification if files need to be retrieved from the backups;

(e) An additional option to ensure that data can be read in the future is to store electronic records in a commonly used format e.g. PDF or XML.

(f) The backup and retrieval software must also be protected to be made available in the event of a disaster;

(g) Backups must be included in disaster recovery plans;

(h) The integrity of backups must be tested using backup test restores and media testing.

17. Verification of Backups

a) Backups will be verified periodically. Logged information generated from each backup will be reviewed daily for the following purposes:

- To check for and correct errors.
- To monitor the duration of backup.
- To optimize backup performance where possible.

b) ICT together with System Administrators will identify problems and take corrective action to reduce any risks associated with failed backups.
c) Random test restores will be done once a month in order to verify that backups have been successful

18. Policy Compliance

A breach of this policy shall have severe consequences and shall be treated in terms of departmental disciplinary code.

19. Review

This policy shall be reviewed every three (3) years and/or when such a need arises.

20. Approval

This policy is approved by the Accounting Officer and is applicable with effect from the date of approval below.

12/10/22

Mr M. MORULE **DATE**

ACTING HEAD OF DEPARTMENT