social development

Department:
Social Development
PROVINCE OF KWAZULU-NATAL

POLICY ON

DATA BACKUP

TABLE OF CONTENTS

1 DEFINITIONS AND ABBREVIATIONS

1.1. **"Application Servers"** means a type of server designed to install, operate and host applications and associated services;

1.2. **"Backup Media"** means a storage device to copy and archive computer data;

1.3. "**Employee**" means any person in the employ of the Department, as defined in terms of Section 1 of the Public Service Act, 1994;

1.4. **"End-User"** means any employee who makes use of, and/or has been issued with, any kind of ICT equipment in the performance of his/her official duties and/or who makes use of network services;

1.5. **"File servers"** means a super computer attached to a network that provides a location for shared disk access;

1.6. **"GITO"** means Government Information Technology Officer;

1.7. **"ICT"** means Information and Communication Technology;

1.8. **"Mail servers"** means a super computer system that sends and receives email;

1.9. **"Server"** means a computer dedicated to running one or more services to serve the needs of users of the computers in the network;

1.10. "**SITA**" means State Information Technology Agency;

1.11. "**Web server**" means a computer system that hosts websites;

2 INTRODUCTION

This policy serves to provide guidelines for the protection of information assets of the Department, whether tangible or intangible. It sets out the control conditions related to the data backup activities within Department.

3 PURPOSE

The purpose of this Policy is to provide guidelines on the preservation, integrity and availability of Department electronic records and ensure restoration of data in the event of data loss.

4 OBJECTIVES

The objective of this policy is to improve the backup plans of information assets for all information systems and personal data in order to facilitate the normal functioning of critical departmental activities in the event of data loss or disaster.

5 SCOPE OF APPLICABILITY

This Policy is applicable to all employees of the Department, contractors and consultants appointed by the department from time to time.

6 LEGISLATIVE FRAMEWORK

6.1 Constitution of the Republic of South Africa, 1996 (Act No.108 of 1996);

6.2 Corporate Governance of ICT Policy;

6.3 Electronic Communications and Transactions Act, 2000 (Act No. 25 of 2000);

6.4 King IV Report on Governance, 2017;

6.5 Minimum Information Security Standards (MISS);

6.6 Protection of Personal Information Act, 2013 (Act No.4 of 2013);

6.7 Public Service Act, 1994 (Proclamation 103 of 1994);

6.8 Public Service Regulations, 2016;

6.9 State Information Technology Agency Act, 1998 (Act No. 88 of 1998); and

6.10 The Regulation of Interception of Communications and Provision of Communication related Information Act 2002 (Act No. 70 of 2002).

7. GUIDING PRINCIPLE

The primary guiding principle is that Department information assets should be preserved and restored in the event of unforeseen data loss or corrupted data (King Report IV on Governance, 2017).

8. POLICY STATEMENTS

8.1 Backup Strategy

A data backup strategy must be developed and maintained and must at the minimum include the following:

8.1.1. Identification of critical data, information and software that needs to be backed up.
8.1.2. The retention periods for backups of critical business process requirements.
8.1.3. The frequency and type of information backup, based on the business requirements.
8.1.4. Action taken in case of temporary or permanent loss; destruction or unavailability of information must be clearly documented, forming a part of the Department's standards and procedures.

8.2 Data Backed Up

Data to be backed up include the following information:

8.2.1. User data stored on the computer hard disk drive.
8.2.2. System user profile.

The following are systems to be backed up

8.2.1.1 File servers.
8.2.1.2 Mail servers.
8.2.1.3 Web server.
8.2.1.4 Application Servers.

8.3 Backup Cycles

The standard backup cycles are daily, weekly and monthly.

8.4 Data Retention

8.4.1 Data retention is the guideline or protocol regarding the saving of data for regulatory or compliance purposes and the disposal of the data when is no longer needed. The classification is detailed as follows:

No.	Information Asset	Retention Period
(I)	The collected data kept by the person who electronically requests, collects, collates, processes or stores the information	As long as information is used,
(II)	A record of any third party.	As long as information is used,.
(III)	All obsolete data.	To be destroyed immediately.

8.4.2 Data backups of systems must be preserved indefinitely as long as the system is still in use by the Department.

8.5 Restoration

The end-user that needs files restored must submit a written request to the ICT help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

8.6 Off-site Storage

8.6.1 Copies of backups must be stored in a safe location, physically distant with at least 80 km away from the primary data processing centre.

8.6.2 To facilitate disaster recovery efforts, off-site storage will be determined by the Head of Department from time to time.

8.7 Testing

Periodic testing of data backup recovery services must be conducted where system owners and end-users confirm successful recovery of data.

8.8 Disposal

8.8.1 Backup media must be physically destroyed in a secure manner that renders the stored data irretrievable.

8.8.2 Media destruction must be conducted by the authorized personnel or an approved designate.

9 GENERAL

9.1 Data Backup Availability

Backup Information must be readily available, but restricted to authorised individuals. In the event where data backup information assets are needed to implement data recovery, these assets must be reliable and available at all times.

9.2 Protection of Data Backups

In accordance with the same Policy, backups must be protected from loss, damage and unauthorised access, by:

9.2.1 Storing them in a fireproof safe on-site to enable important information to be restored promptly;
9.2.2 Supporting them by copies kept off-site to enable required data to be restored using alternative location in case of a disaster; and
9.2.3 Restricting access to authorised personnel.

10 NON COMPLIANCE

An employee who fails to comply with this Policy shall be guilty of an act of misconduct.

11 MONITORING, EVALUATION AND REVIEW

11.1. GITO is responsible for communicating the provisions of this Policy to all Employees.

11.2. The Policy will be monitored, evaluated and reviewed after three (3) years or as and when the need arises.

12 EFFECTIVE DATE

The Policy is effective from the date of approval by the Head of Department.

13 TITLE OF THE POLICY

This Policy must be called the Policy on Data Backup.

14 POLICY APPROVAL

14.1. This Policy supersedes all other policies already in existence.

14.2. The revised Policy is approved with effect from the 05th day of November in the year 2018.

05/11/2018

MS. N.G. KHANYILE
HEAD OF DEPARTMENT
DEPARTMENT OF SOCIAL DEVELOPMENT

DATE