C. Backup Policy

I. Definition and Terms

Terms	Definition
i) Archive	the process of **moving** inactive files from online disk storage to tape, i.e. deleting the files from disk after copying them, in order to release online storage for re-use
ii) Backup	the process of **copying** active files from online disk storage to tape so that files may be restored to disk in the event of damage to or loss of data
iii) Backup administrator	a person designated to perform the administration functions and maintenance of the backup solution
iv) Backup tape	the tape storage media where the information is to be stored for offline and/or offsite storage
v) File server	A device which controls access to separately stored files, as part of a multi-user system
vi) Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria.
vii) Mail server	An application that receives incoming email from local users and forwards outgoing email for delivery
viii) Active Directory controllers	Server running a version of windows server operating system and has the service of active directory installed.
ix) Department	the Department of Social Development
x) End user	the person utilising the information
xi) Grandfather- Father-Son (GFS)	a tape rotation strategy. GFS simplifies tape handling by organizing rotation into daily, weekly, and monthly backup tapes. You can also create Custom backup jobs that use the GFS strategy
xii) Server	A computer or device on a network that manages network resources or provides services and resources to users.
Acronyms	
i) LAN	Local Area Network
ii) WAN	Wide Area Network
iii) CFO	Chief Financial Officer

iv) SG	Superintendent General
v) ECDSD	Social Development Eastern Cape
vi) IT	Information Technology
vii) ISO	International Standard of Operation

II. Legislative Framework

i) Minimum Information Security Standard (MISS)
ii) Public Finance Management Act (PFMA)
iii) Public Service Regulation (PSR 2008)
iv) Public Service Act (Act No. 103 of 1994)
v) Labour Relations Act (Act No.12 of 2002)
vi) ISO 27001: (2005)
vii) Electronic and Communication and Transaction Act (Act No. 25 of 2002)
viii) Regulation of Interception of Communication Act (Act No. 70 of 2002)
ix) Protection of Information Act (Act No. 84 of 1982)
x) Protection of Personal Information (Act No 4 of 2013)
xi) Disaster Recovery Policy (2016)
xii) Disaster Recovery Plan (2016)
xiii) CIO Charter (2013)

1. Preamble

The policy has been in use since 2012 but was due for review as it was in its third year of implementation. This document provides a standard guideline to ensure that Department of Social Development data can be fully recovered in case of accidental, intentional corruption or deletion. The most fundamental aspect of storage management is therefore the access, backup and recovery process. Managing huge quantities of diverse data, widely distributed across the enterprise is a daunting task. Technology, when integrated into a comprehensive data and business recovery strategy, can reduce the risk of data loss and reduce the cost of data recovery and downtime.

The rapid development and progress in the area of computer technology add to the escalating threat in respect of information systems security, which calls for the establishment of security policies, standards and control measures to protect the information systems configurations and information of the ECDSD against security risks. This policy is based on international standards, best practices, South African government law, regulation and acts and is subject to the policies and standards as issued by National Intelligence regarding minimum information security standards

Executive management acknowledges the importance of the computing resources of the ECDSD and supports information systems security throughout the department. This policy should be read in conjunction with the Disaster Recovery Plan and Policy.

2. Purpose

This document is to define and provide a framework for managing data storage and focusing on efficient and dependable archival, preservation and retrieval of information leveraged by applications and employees of the Department of Social Development.

3. Objective

a) This document provides a standard guideline to ensure that Department of Social Development data can be fully recovered in case of accidental, intentional corruption or deletion.

b) Provide proper controls and management systems that will ensure effective, efficient and economical use of the ECDSD's information.

4. Scope of Applicability

This policy applies to the backup administrator who administer any ECDSD-owned internal network domain servers or otherwise.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting departmental information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy Provisions

The policy seeks to provide the following provision:

a) Controls shall be established that must ensure proper management of risks associated with ownership and safeguarding of information which includes:
   i) implement and enforce storage of department approved information on enterprise computers and servers. This ensures that data such as music files, and picture files, do not take space on enterprise storage facilities;
   ii) enforce centralised storage of documents on LAN servers (preferably with offline folder synchronisation for mobile laptops) to facilitate centralised data backup; and
   iii) implement a well-documented tape rotation system to safeguard against accidental overwriting of tapes.

b) Advanced scheduling, automated unattended operation, centralised reporting, and enterprise-wide media management shall be performed;

c) high-performance backup and restore features that reduce the backup window shall be implemented to improved availability of data;

d) Ensure that backup procedures adhere to international standards and procedures;

e) Ensure that in the event of a disaster, backup files can be recovered:
   i) implement scheduled unattended but auditable backup systems that allow operation when network traffic on the enterprise network is at a minimum; and
   ii) implement a backup solution that minimises the recovery time for information by allowing selective restoration.

g) Ensure data integrity at all times by monthly testing the backed up information;

h) Ensure offsite storage is maintained at all times to enable recovery of information should a disaster occur (onsite) due to fire, floods or other causes;

i) Ensure that backup tapes/cassettes are labelled according to the prescribed procedures:
   i) implement a regularly scheduled data restoration exercise to ensure back media is recoverable; and
   ii) keep backups on storage tape offsite to avoid being destroyed should a disaster occur onsite.

j) Ensure all changes to strategy, policy and procedures are properly authorised and documented:

   i) maintain a change control register to record all changes to the policy and procedures; and

   ii) ensure the correct authorisation is obtained prior to effecting any changes.

6.1 Tape Storage

a) There shall be a separate or set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday;

b) Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week;

c) There shall be a separate or set of tapes for each Friday of the month such as Friday1, Friday2, etc.

d) Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday.

e) Every month a monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets or archived as the monthly backups and for each Fridays a new set of tapes used.

6.2 Tape Drive Cleaning

a) Tape drives shall be cleaned weekly and the cleaning tape shall be changed according to manufacture specification.

6.3 Age of tapes

a) The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes.

6.4 Data to be Backed Up

Data to be backed up include the following information:

a) Official User data residing on official laptops and desktops.

Systems to be backed up include but are not limited to:

a) File server;

b) Mail server;

c) Production database server;

d) Active Directory controllers;

6.5 Constraints and special considerations

a) Tape devices will be required at remote servers to cater for remote servers for local remote server backup;

b) Offline folder synchronisation for desktops and laptops is required to facilitate local remote data centralisation for remote sites;

c) **Firewall:** care must be taken to ensure the backup traffic is allowed through.

7 Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Backup Policy

8 Accountabilities and Responsibilities

8.1 The Superintendent General

The SG working in conjunction with the CIO shall be responsible for ensuring the effective implementation and compliance of the ECDSD policies, standards and procedures.

8.2 Asset/information/application owner

c) The designated owner of the information asset shall take responsibility for all access granted.

d) The owner of the information resource shall ensure that all access to the resource granted is appropriate and justified.

8.3 Data Warehouse Manager

The Data Warehouse Manager is also responsible for maintaining this policy.

8.4 Internal Audit

c) The Internal Audit department is authorised by management to assess compliance with all departmental policies at any time.

d) The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to access to ECDSD environment.

8.5 Backup admin

The backup administrators' responsibilities are to:

a) swap the tapes;

b) transfer tapes to offsite storage as per the tape rotation policy;

c) check backup job status;

d) complete the Backup Log daily;

e) ensure that backup and storage logs are maintained;

f) escalate backup issues;

g) ensure that all tapes are write-enabled before inserting into the tape drive;

h) ensure that all tapes are marked properly, i.e. with the name of the type of backup, as well as the date when the tape is used for backup and the save set name is written into the backup logbook next to the appropriate tape;

i) on completion of a backup, the operator must enter the backup date and tape numbers onto the Backup Logbook as well as the backup on the label supplied in tape's case; and

j) store backup tapes in a safe before they are collected to be stored off site.

Failure to execute the above responsibilities must be viewed as negligence and can result in severe data loss.

9 Effective date of the Policy

The Backup Policy is effective upon the date the member of the Executive Council has approved it.

10 Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) VEEAM Backup System

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy:

11 Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12 Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Access Control Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

d) ensure that backup and storage logs are maintained;

e) escalate backup issues;

f) ensure that all tapes are write-enabled before inserting into the tape drive;

g) ensure that all tapes are marked properly, i.e. with the name of the type of backup, as well as the date when the tape is used for backup and the save set name is written into the backup logbook next to the appropriate tape;

h) on completion of a backup, the operator must enter the backup date and tape numbers onto the Backup Logbook as well as the backup on the label supplied tape's case; and

i) store backup tapes in a safe before they are collected to be stored off site.

Failure to execute the above responsibilities must be viewed as negligence and can result in severe data loss.

13 Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/ March 2016
Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016.
Date

Annex A : Procedures for backup

A.1 Backup schedule and tape rotation

The ECDSD's backup solution uses a four-daily, four-weekly and one-monthly Grandfather-Father-Son data retention cycle. A **Grandfather-Father-Son** rotation scheme must be operated; incremental daily backups *(Son)* must run overnight from Monday to Thursday and must be rotated on a three or four week basis. A full weekly backup (the **Fathers**) must run on Fridays of each week and one full backup per month (the **Grandfather**) must run and be kept for 12 months.

The following data retention cycle must be used when performing backups:

1. Daily GFS data retention cycle:
   - i) ***Server/application/database*-MON-DATE**
   - ii) ***Server/application/database* -TUE-DATE**
   - iii) ***Server/application/database* -WED-DATE**
   - iv) ***Server/application/database* -THU-DATE**

b) Weekly GFS data retention cycle:
   - i) **Week1 – *Server/application/database* -FRI-DATE**
   - ii) **Week2 – *Server/application/database* -FRI-DATE**
   - iii) **Week3 – *Server/application/database* -FRI-DATE**
   - iv) **Week4 – *Server/application/database* -FRI-DATE**
   - v) **Week4 – *Server/application/database* -FRI-DATE**
   - vi) **Week5 – *Server/application/database* -FRI-DATE**

c) 12-monthly GFS data retention cycle:
   - i) **January09 - *Server/application/database* -JAN-DATE**
   - ii) **February09 - *Server/application/database* -FEB-DATE**
   - iii) **March 09 till - *Server/application/database* -MAR-DATE**
   - iv) **December09 - *Server/application/database* -DEC-DATE**

During week one, the Week1 set is used and during week two, Week2 set is used and so on.

The following schedule is used for daily and weekly tape rotation:

Monday (or first business day of the week):

Deliver the previous week's **weekly tape** to the offsite storage facility and collect the oldest set of weekly tapes, e.g. (if you were using Week1 last week you need to send the tapes to the offsite storage and bring the Week2 tapes to the offices).

Make sure that you run a device inventory once the tape has been inserted into the Tape library.

Place the old weekly set in the fire-proof safe and insert new weekly's tape in the tape library. Your tape is now ready for the backup in the evening of that day.

Also note that all daily tapes and 2 spare tapes must be kept in the tape library and these can be changed over a longer period of time. Weekly tapes must be changed

every Monday of the week and monthly Tapes must be changed every first Monday of the Month at 10h00 am.

It is therefore preferable to do this in the morning so that it becomes a routine. Backups only run at 19:00 so that all data for the day is captured on the tapes.

The following schedule is used for monthly tape rotation:

The tapes in this must be labelled:

January

February

March

April

May

June

July

August

September

October

November

December

On the last business day of the month, the daily or weekly backup tape must not be used. Instead use the monthly tape corresponding with the month that you are in. This tape must be taken to the offsite storage as soon as possible. **Note: These tapes should never be kept onsite; they can only be used for emergency recovery.**

A.2 Checking backup job and completion of backup log

As part of the daily backup job the tape will be ejected from the Tape drive into the Tape library after the backup has completed. If the tape has not ejected by 08:00 in the morning there could be an issue with the backups; notify the backup administrators.

Backup job status will be e-mailed to the backup administrators immediately after the job completion. This e-mail is to be used to complete the backup log as it will have information on whether the backup job completed successfully or failed. A detailed log file will also be attached to the e-mail.

The technicians are not allowed to modify any jobs; it is the responsibility of the backup administrators to modify backup scripts. The log file can be forwarded to the backup administrator who will be able to identify the cause of the failed/incomplete backup.

Backup administrators must make sure that each backup tape is labelled stating the specific backup name and serial number. Both the tape and case must be labelled and it is the responsibility of the backup administrator to replace broken or faulty tapes. He/she must also make sure that all backup logs are analysed and resolved if there are any backup issues that are reported.

There are four types of backups logs that the ECDSD will be utilising, viz.

Backup log: This log must be created and maintained by the backup software and stored on the backup tape and on the hard drive. The Backup Log is used to monitor the swapping

of tapes and the status of the backups. This needs to be completed every morning when the tapes are swapped. The log file must also be printed and kept in a file in the fire-proof safe. A page will exist for every month and the backups are logged against the sheet.

Error log: This log must be created and maintained by the backup software and stored on the backup tape and on the hard drive.

Backup Restore Log: This log will be created and maintained by the backup software and stored on the backup tape and on the hard drive.

Backup Storage Log: A logbook will be kept at the on-site and off-site storage location. The following backup schedule must be adhered to.

Monday	Tuesday	Wednesday	Thursday	Friday
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup

The following is an example of the backup log.

ECDSD Backup Log			Month/Year:			
DATE	TAPE NAME	Tape Serial#	JOB STATUS	ON FAILED/INCOMPLETE STATUS; WHAT ACTION WAS TAKEN	BACKUP ADMIN	SIGNATURE

This log must be completed and signed by the relevant Backup Admin as a log to the completion of the backups. The updates to this log are just as critical as the tapes being swapped and are used when recovery of data is required.

A.3 Backup admin responsibilities and delegation

The backup administrators' responsibilities are to:

a) swap the tapes;

b) transfer tapes to offsite storage as per the tape rotation policy;

c) check backup job status;

d) complete the Backup Log daily;