



ICT DATA BACKUP AND RECOVERY POLICY

Date
Approved: **30/08/2023**

Council
Resolution: **E.6/08/2023**

TABLE OF CONTENTS

1.	INTRODUCTION	4
2.	LEGISLATIVE FRAMEWORK	4
3.	OBJECTIVE OF THE POLICY	5
4.	AIMS OF THE POLICY	5
5.	SCOPE.....	5
6.	BREACH OF POLICY	5
7.	ADMINISTRATION OF POLICY	5
8.	DATA BACKUP STANDARDS	6
9.	DATA BACKUP SELECTION	6
10.	BACKUP TYPES	6
11.	BACKUP SCHEDULE	7
12.	DATA BACKUP PROCEDURES	7
13.	STORAGE MEDIUM	9
14.	DATA BACKUP OWNER.....	9
15.	OFFSITE STORAGE SITE.....	9
16.	TRANSPORT MODES	10
17.	RETENTION CONSIDERATIONS.....	10
18.	RECOVERY OF BACKUP DATA	10
19.	THE ROLE OF BACKUPS IN RECORDS MANAGEMENT	11
20.	GENERAL RULES FOR RETENTION PERIODS	12
21.	REFERENCES.....	16

Glossary of Abbreviations

Abbreviation	Description
AD	Active Directory
HR	Human Resources
UI	User Information
LTO	Linear Tape Open

Glossary of Terminologies

Terminology	Definition
Ad hoc	As and when requested.
Availability	The proportion of time a system is in a functioning condition.
Backup time window	Time slot during a 24hour day that backups are allowed to run in.
Critical data	Data that is required to be retained for a set period as determined by law, or data that can severely disrupt services when lost. Examples include: financial data, client personal data etc.
Data medium	Medium on which backups are stored egg. Tapes, hard disks, CD/DVD, Hard disk repository.
Data referencing	Data that defines the set of permissible values to be used by other data sets.
Downtime	Defined as the periods when a system is unavailable.
Generations	Structural term designating the grandfather-father-son (Full-differential-incremental) backup relationship.
Integrity	Data integrity is defined as is the assurance that data is consistent and correct.
Pseudo generation	Randomly created.
Storage capacity	Amount of space (Tb; Gb; Mb) utilized.

1. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access (see ICT User Access Management Policy for further detail), manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data. It seeks to define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, 1996.
- Copyright Act, Act No. 98 of 1978
- Electronic Communications and Transactions Act, Act No. 25 of 2002
- Minimum Information Security Standards, as approved by Cabinet in 1996
- Municipal Finance Management Act, Act No. 56 of 2003
- Municipal Structures Act, Act No. 117 of 1998
- Municipal Systems Act, Act No. 32, of 2000
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996
- National Archives Regulations and Guidance
- Promotion of Access to Information Act, Act No. 2 of 2000
- Promotion of Administrative Justice Act, Act No. 3 of 2000
- Protection of Personal Information Act, Act No. 4 of 2013
- Regulation of Interception of Communications Act, Act No. 70 of 2002
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014
- Control Objectives for Information Technology (COBIT) 5, 2012

- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles, 2009

3. OBJECTIVE OF THE POLICY

The primary objective of the policy is to protect the Municipality's data. This policy seeks to outline the data backup and recovery controls for Municipal employees so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice.

4. AIMS OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to a standard backup and recovery control process in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency.

5. SCOPE

This ICT Data Backup and Recovery Policy has been created to guide and assist the Municipality to align with internationally recognised best practices, regarding data backup, recovery controls and procedures. This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

The policy applies to everyone in the Municipality, including its service providers and consultants. This policy is regarded as crucial to the effective protection of data, of ICT systems of the Municipality.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any employee or service provider, who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy; or
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
- Punitive recourse against a service provider.

7. ADMINISTRATION OF POLICY

The ICT Manager is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and changes approved by the Council.

8. DATA BACKUP STANDARDS

- 8.1 Critical data, which is critical to the Municipality, must be defined by the Municipality and must be backed up. Critical data must also include cloud storage.
- 8.2 Backup data must be stored at a location that is physically different from its original creation and usage location.
- 8.3 Data restores must be tested weekly.
- 8.4 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) A definition of the 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.
- 8.5 Data Backup notifications must be computerized in the event of failure or success.

9. DATA BACKUP SELECTION

- 9.1 All data and software essential to the continued operation of the Municipality, as well as all data that must be maintained for legislative purposes, must be backed up.
- 9.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
- 9.3 The application owner, together with the ICT Manager, will determine what information must be backed up, in what form, and how often.

10. BACKUP TYPES

- 10.1 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. This statement will need to be reviewed once the ICT DR Business Impact and Risk Analysis requirements are updated with input from Line Managers and Municipal operations.

- 10.2 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.
- 10.3 In the event that a system requires a high degree of skill to recover 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.

11. BACKUP SCHEDULE

- 11.1 Choosing the correct Backup Schedule:
 - (a) Backup schedules must not interfere with day to day operations. This includes any end of day operations on the systems.
 - (b) A longer backup window might be required, depending on the type of backups chosen.
- 11.2 Frequency and time of data backup:
 - (a) 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.
 - (b) Immediate full data backups are recommended when data is changed to a large extent or the entire database needs to be made available at certain points in time. Regular, as well as event-dependent intervals, need to be defined.
- 11.3 Previous versions:
 - (a) The previous two versions of operating systems and applications must be retained at the off-site storage location.
 - (b) Annual, quarterly, monthly and weekly backups must be retained at the off-site facility. Monthly backups may be re-used to take new backups, when annual backups are successfully taken.

12. DATA BACKUP PROCEDURES

- 12.1 The ICT Manager/team 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 Backups	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.

12.2 The ICT Manager/team must choose between centralized and decentralized 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
Centralized Backups	The storage location and the performance of the data backup are carried out on a central ICT system by a small set of trained administrators.	Allows for more economical usage of data media.	There is added exposure to confidential data. Confidential and non-confidential information may be combined requiring more stringent security controls for handling the backups.
Decentralized Backups	Performed by ICT users or administrators without being transferred to a central ICT system.	ICT users can control the information flow and data media, especially in the case of confidential data.	The consistency of data backup depends on the reliability and skill level of the user. Sloppy procedures can result in data exposure or loss.

13. STORAGE MEDIUM

- 13.1 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) Storage capacity;
 - (c) Rate of increasing data volume;
 - (d) Cost of data backup procedures and tools vs. cost if restored without backup;
 - (e) Importance of data;
 - (f) Life and reliability of data media;
 - (g) Retention schedules; and
 - (h) Confidentiality and integrity.
- 13.2 Should high availability be required, a compatible and fully operational reading device (e.g. tape drive, CD, DVD) must be obtainable on short notice to ensure that the data media is usable for restoration even if a reading device fails for historical backups.

14. DATA BACKUP OWNER

- 14.1 The ICT Manager must ensure that two employees (One primary, one secondary) are delegated to commit and adhere to each backup schedule.

15. OFFSITE STORAGE SITE

- 15.1 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.
- 15.2 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.
- 15.3 Should high availability be required, additional backup copies should be stored in the immediate vicinity of the ICT system.
- 15.4 Minimum requirements are to store the weekly, monthly, quarterly and or yearly backup sets off site.
- 15.5 The site used for storing data media off-site must meet Physical Security requirements defined within the ICT Security Controls Policy
- 15.6 Weekly, monthly and quarterly backups must be stored offsite for the entire duration of the retention period.

- 15.7 Receipts of media being collected and delivered must be kept for record keeping purposes and must be signed by ICT staff in attendance.
- 15.8 Should an off-site media set be required to perform a restore, the data media must be returned to the offsite facility for the remainder of the retention period
- 15.9 All data media used to store confidential information must be disposed of in a manner that ensures the data is not recoverable.

16. TRANSPORT MODES

- 16.1 When choosing the transport mode for the data (logical or physical), it is important to consider the following:
 - (a) Time constraints;
 - (b) Capacity requirements; and
 - (c) Security and encryption.

17. RETENTION CONSIDERATIONS

- 17.1 Data should be retained in line with current legislative requirements, as defined in sections 19 and 20 of this document.
- 17.2 An example of 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) Quarterly Backups will be saved for one year thus every 4th quarter afterwards it can be recycled.
 - (e) Yearly backups will be retained for five years and will only be run once a year at a predetermined date and time.
 - (f) 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.

18. RECOVERY OF BACKUP DATA

- 18.1 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.
- 18.2 Documentation of the restoration process must include:
- (a) Procedures for the recovery
 - (b) Provision for key management should the data be encrypted.
- 18.3 Recovery procedures must be tested at least monthly.
- 18.4 Recovery tests must be documented and reviewed by the ICT Manager.

19. THE ROLE OF BACKUPS IN RECORDS MANAGEMENT

- 19.1 The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions.
- 19.2 The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the Municipality. The Records Manager is also responsible for maintaining the retention periods indicated on the file plan and disposal schedule.
- 19.3 The ICT Manager must work with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.
- 19.4 Backups are not ideal, but not excluded, as a means of electronic record and e-mail retention for the prescribed periods. It is difficult to implement a proper file plan using backup media and therefore it is difficult to arrange, retrieve and dispose of records.
- 19.5 The role of backups in records management is more suited as a means to recover electronic records management systems and e-mail systems in the event of a disaster or technology failure.
- 19.6 The ICT Section is responsible for the following, when backing up electronic records or e-mails that are regulated under the National Archives and Records Service of South Africa Act:
- (a) Backups must be made daily, weekly, monthly, quarterly and yearly;
 - (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 scheme if files need to be retrieved from the backups;
 - (e) Backups must survive technology obsolescence by migrating them to new hardware and software platforms when required. An additional option to ensure that data can be read in the future is to store electronic records and e-mails in a commonly used format e.g. PDF or XML.

- (f) The backup and retrieval software must also be protected to be 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.
- 19.7 The ICT Manager must ensure that systems prevent the deletion of electronic records or e-mails without consulting the Records Manager.
- 19.8 The ICT Manager and Records Manager must implement the most practical method to retain e-mails e.g. file inside e-mail application, transmit to document management solution, transfer to e-mail archiving solution, save to shared network drive, print to paper etc.
- 19.9 Officials are responsible for filing e-mails. It is the responsibility of the sender or their designated official to file e-mails unless the e-mail is received from outside in which case the recipient or designated official is responsible for filing it.
- 19.10 The Records Manager must create awareness with Officials of the importance of e-mail as public records. This include, but are not limited to:
- (a) E-mails must be properly contextualised and meaningful over time;
 - (b) Subject lines are very important and must be descriptive;
 - (c) The reference number of the subject folder in the file plan must be included in the top right hand corner of the message box;
 - (d) Auto-signatures must be used and shall contain full details of the sender; and
 - (e) Attachments must be filed into the file plan in the document management system before it is attached to the e-mail.
- 19.11 The ICT manager must ensure that the e-mail system is set up to capture the sender and the recipient(s), and the date and time the message was sent and/or received. When an e-mail is sent to a distribution list, information identifying all parties on the list must be retained for as long as the message is retained.
- 19.12 The Records Manager may dispose of any electronic records and e-mails if retention is not required under any Act or General Disposal Authority.

20. GENERAL RULES FOR RETENTION PERIODS

- 20.1 The National Archives provides the primary considerations when defining retention periods of electronic records and e-mails. This also supports the goals of the Promotion of Administrative Justice Act. This supports the goals of the Promotion of Administrative Justice Act, Act. No. 3 of 2000, which is to ensure that public records are available as evidence to ensure that administrative action is lawful, reasonable and procedurally fair.

Act or National Archive Regulations and Guidance	Item	Retention period
National Archives and Record Service of South Africa Act, Act No. 43 of 1996 Promotion of Administrative Justice Act, Act No. 3 of 2000	Public records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions.	Records may not be disposed of unless written authorisation have been obtained from the National Archivist or a Standing Disposal Authority have been issued by the National Archivist against records classified against the file plan.
General Disposal Authority PAP1 Disposal of personal files of local authorities	Personal case files of local authorities	At the discretion of the Municipality, taking into consideration any special circumstances.
General Disposal Authority No. AE1 for the destruction of ephemeral electronic records and related documentation	Electronic records with no enduring value	16 Categories of records. Refer to AE1 for details.
General Disposal Authority No. AT2 on the destruction of transitory records of all governmental bodies	Electronic records not required for the delivery of services, operations, decision-making or to provide accountability	Refer to AT2 for details.

Act or National Archive Regulations and Guidance	Item	Retention period
Managing electronic records in governmental bodies Policy, principles and requirements Managing electronic records in governmental bodies Metadata requirements	E-mails, and attachments therein, must be retained if they: <ul style="list-style-type: none"> • Are evidence of Municipal transactions; • Approve an action, authorize an action, contain guidance, advice or direction; • Relate to projects and activities being undertaken, and external stakeholders; • Represent formal business communication between staff; or • Contain policy decisions. 	E-mails fall into one of the 4 categories above and must be retained as such.

20.2 Public records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions may not be destroyed until such time that the Legal Services Manager has indicated that the destruction hold can be lifted.

20.3 The Municipal Finance Management Act, No 56. of 2003, Section 62 1)b) states that Municipal records must be retained in the manner prescribed by legislation. However, the Act does not specify retention periods. National and Provincial retention periods for financial records are prescribed within Treasury Regulations, Regulation 17 to the Public Finance Management Act, No. 1 of 1999, Section 40(1)(a). For the purposes of this policy, the Treasury Regulations, Regulation 17, will be used as guidance only without intervening National Archivist legislation, regulations and guidance.

Act or National Archive Regulations and Guidance	Item	Retention period
Treasury Regulations, Regulation 17	Internal audit reports, system appraisals and operational reviews.	10 years

Act or National Archive Regulations and Guidance	Item	Retention period
Treasury Regulations, Regulation 17	Primary evidentiary records, including copies of forms issued for value, vouchers to support payments made, pay sheets, returned warrant vouchers or cheques, invoices and similar records associated with the receipt or payment of money.	5 Years
Treasury Regulations, Regulation 17	Subsidiary ledgers, including inventory cards and records relating to assets no longer held or liabilities that have been discharged.	5 Years
Treasury Regulations, Regulation 17	Supplementary accounting records, including, for example, cash register strips, bank statements and time sheets.	5 Years
Treasury Regulations, Regulation 17	General and incidental source documents not included above, including stock issue and receivable notes, copies of official orders (other than copies for substantiating payments or for unperformed contracts), bank deposit books and post registers.	5 Years

- 20.4 In accordance with Treasury Regulations, Regulation 17(2), financial information must be retained in its original form for one year after the financial statements and audit report has been presented to the Council.
- 20.5 Financial information may be stored in an alternative form, after expiry of one year from submission of the financial statements to the Council, under the following conditions:
- (a) The records must be accessible to users. This requires data referencing, a search facility, a user interface or an information system capable of finding and presenting the record in its original form.
 - (b) The original form may have reasonable validations added, which is required in the normal course of information systems communication, storage or display.
- 20.6 The Electronic Communication and Transaction Act, No 25 of 2005 regulates the storage of personal information.

21. REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

Electronic Communications and Transactions Act, No. 25. (2002). Republic of South Africa.

King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.

Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.

Minumum Information Security Standards. (1996, December 4). Cabinet.

Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.

Treasury Regulations for departments, trading entities, constitutional institutions and public entities. (2005, March). National Treasury, Republic of South Africa.

National Archives and Records Service of South Africa Act, No. 43 of 1996