



ICT DATA BACKUP AND RECOVERY POLICY

1 July 2024

Table of Contents

1. ABBREVIATIONS	2
2. PURPOSE OF THE POLICY	3
3. LEGISLATIVE FRAMEWORK	4
4. USER AWARENESS	4
5. SCOPE	5
6. DATA BACKUP STANDARDS.....	5
7. DATA BACKUP SELECTION	6
8. BACKUP TYPES.....	7
9. BACKUP SCHEDULE	7
10. DATA BACKUP PROCEDURES	8
11. STORAGE MEDIUM.....	9
12. DATA BACKUP OWNER	9
13. OFFSITE STORAGE SITE	10
14. TRANSPORT MODES.....	11
15. RETENTION CONSIDERATION	11
16. RECOVERY OF BACKUP DATA.....	11
17. BACKUPS IN RECORD MANAGEMENT	12
18. GENERAL RULES FOR RETENTION PERIODS	15
19. BACKUP STRATEGY	19
20. BACKUP DESIGN PRINCIPLES	20
21. SYSTEMS PROTECTION STRATEGY	21
22. BREACH OF THIS POLICY	23
23. POLICY REVIEW	24

1. ABBREVIATIONS

“**AD**” refers to the active directory.

“**ICT**” refers to Information Communication Technology.

“**IT**” refers to Information Technology.

“**ICTCOM**” refers to the ICT Steering Committee.

“**SWDM**” refers to Swellendam Municipality.

“**Municipality**” refers to the Swellendam Municipality.

“**email**” refers to electronic mail.

“**MM**” refers to the Municipal Manager.

“**Site Manager**” refers to the service provider appointed to provide technical support.

“**Manager ICT Services**” refers to the Head of the ICT Services Division.

“**CFO**” refers to the Chief Financial Officer or Director Financial Services.

“**SCM**” refers to Supply Chain Management.

“**HR**” refers to Human Resource Management.

“**Users**” refers to Councillors, Employees, End Users, Interns, Temporary Staff Members and Contract Workers.

“**Manager**” refers to the Head of each Division.

“**Network Devices**” refers to computers and devices interconnected by communications channels that facilitate communications among users.

“**IR**” refers to the Information Resources.

“**SLA**” refers to Service Level Agreement.

“**Workstations**” refers to computers, laptops, printers and photocopiers.

“**VPN**” refers to Virtual Private Network.

“**ISO**” refers to International Organization for Standardization.

“**POPIA**” refers to the Protection of Personal Information Act.

2. PURPOSE OF THE POLICY

- 2.1 Information security is becoming increasingly important to the SWDM, driven in part by changes in the regulatory environment and advances in technology.
- 2.2 Information security ensures that the SWDM ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as the unauthorised disclosure or incorrect processing of data.
- 2.3 The Backup procedure is responsible for ensuring that all municipality data stored on approved systems within the SWDM environment is recoverable in the event of accidental loss or damage.
- 2.4 The purpose of the policy is to protect the SWDM data. This policy seeks to outline the data backup and recovery controls for Municipal employees to ensure that the data is correctly and efficiently backed up and recovered in line with best practices.
- 2.5 The policy must ensure that the SWDM 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, and service efficiency.
- 2.6 In addition, 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.

3. LEGISLATIVE FRAMEWORK

- 3.1 The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.
- 3.2 The following legislation, among others, was considered in the drafting of this policy:
- 3.2.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
 - 3.2.2 Copyright Act, Act No. 98 of 1978
 - 3.2.3 Electronic Communications and Transactions Act, Act No. 25 of 2002
 - 3.2.4 Minimum Information Security Standards, as approved by Cabinet in 1996
 - 3.2.5 Municipal Finance Management Act, Act No. 56 of 2003
 - 3.2.6 Municipal Structures Act, Act No. 117 of 1998
 - 3.2.7 Municipal Systems Act, Act No. 32, of 2000
 - 3.2.8 National Archives and Record Service of South Africa Act, Act No. 43 of 1996
 - 3.2.9 National Archives Regulations and Guidance
 - 3.2.10 Promotion of Access to Information Act, Act No. 2 of 2000
 - 3.2.11 Promotion of Administrative Justice Act, Act No. 3 of 2000
 - 3.2.12 Protection of Personal Information Act, Act No. 4 of 2013
 - 3.2.13 Regulation of Interception of Communications Act, Act No. 70 of 2002
 - 3.2.14 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.
- 3.3 The following internationally recognised ICT standards were leveraged in the development of this policy:
- 3.3.1 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
 - 3.3.2 Control Objectives for Information Technology (COBIT) 5, 2012
 - 3.3.3 ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
 - 3.3.4 King Code of Governance Principles IV, 2009

4 USER AWARENESS

- 4.1 Every councillor, employee, contractor and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of

adhering to it when using the Municipality's computers, networks, data and other information resources. Each user is responsible for reporting any suspected breaches of this policy's terms to the Manager: ICT Services.

- 4.2 The contents of this policy will be made available through presentations to all staff members and all those who attend must sign an attendance register and/or email and/or place it on the SWDM Network.

5 SCOPE

- 5.1 This ICT Data Backup and Recovery Policy have been created to guide and assist the SWDM 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.
- 5.2 The policy applies to everyone in the SWDM, including its service providers and consultants. This policy is regarded as crucial to the effective protection of data, of ICT systems of the SWDM.
- 5.3 SWDM must develop their own Data Backup and Recovery controls and procedures by adopting the principles and practices put forward in this policy.

6 DATA BACKUP STANDARDS

- 6.1 Critical data, which is critical to the SWDM, must be defined by the municipality in consultation with ICT and must be backed up.
- 6.2 Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site).

The medium will dictate when scheduled. (To be implemented when disaster recovery site is established).

- 6.3 Data restores must at least be tested quarterly.
- 6.4 Procedures for backing up critical data and the testing of the procedures must be documented by the ICT Services Division. These procedures must include, as a minimum, for each type of data and system:
 - 6.4.1 A definition of the specific data to be backed up;
 - 6.4.2 The type(s) of backup to be used (e.g. full backup, incremental backup, etc.);
 - 6.4.3 The frequency and time of data backup;
 - 6.4.4 The number of generations of backed-up data that are to be maintained (both on-site and off-site);
 - 6.4.5 Responsibility for data backup;
 - 6.4.6 The storage site(s) for the backups;
 - 6.4.7 The storage media to be used;
 - 6.4.8 Any requirements concerning the data backup archives;
 - 6.4.9 Transport modes; and
 - 6.4.10 Recovery procedure of backed-up data.

7 DATA BACKUP SELECTION

- 7.1 All data and software essential to the continued operation of the SWDM, as well as all data that must be maintained for legislative purposes, must be backed up.
- 7.2 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.

- 7.3 The application owner, together with the ICT, will determine what information must be backed up, in what form, and how often.

8. BACKUP TYPES

- 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.
- 8.2 Once a month, a full backup should be stored off-site. This statement will be subject to the review of the ICT Disaster Management Policy and is updated with input from System Administrators, Line Managers and Municipal operations. (Currently, only SAMRA'S is stored offsite. Once disaster Recovery is implemented the rest of the backups will be stored offsite.)
- 8.3 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.
- 8.4 If a system requires a high degree of skill to recover from backup, consideration must be given to making full images of such servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.
- 8.5 For monitoring purposes, the ICT Manager must create a summary of backup types, along with their advantages, disadvantages and frequency.

9. BACKUP SCHEDULE

- 9.1 Choosing the correct Backup Schedule:
- 9.1.1 Backup schedules must not interfere with day-to-day operations. This includes any end-of-day operations on the systems.
- 9.1.2 A longer backup window might be required, depending on the type of backup.

- 9.2 Frequency and time of data backup:
 - 9.2.1 When the data in a system changes frequently, backups need to be taken more frequently to ensure that data can be recovered in the event of a system failure.
 - 9.2.2 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.
- 9.3 Previous versions:
 - 9.3.1 The ICT Manager should determine the number of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location.
 - 9.3.2 Annual, monthly and weekly backups must be retained at the Backup and Disaster Recovery location. Weekly, Monthly and Annual backup media may be re-used to take new backups. (To be implemented when disaster recovery site is established.)

10. DATA BACKUP PROCEDURES

- 10.1 The ICT Manager in collaboration with the CFO must choose between automated and manual backup procedures based on their requirements and constraints. Both procedures are in line with best practices.
- 10.2 The ICT Manager in collaboration with the CFO must choose between centralized and decentralized backup procedures based on their requirements and constraints. Both procedures are in line with best practices.
- 10.3 The ICT Manager must submit quarterly to the ICTCOM the register of backups taken, the frequency and which procedure was done and where the backups were stored.

11. STORAGE MEDIUM

- 11.1 When choosing the data media format for backups, it is important to consider the following:
- 11.1.1 Time constraints around identifying the data and making the data available;
 - 11.1.2 Storage capacity;
 - 11.1.3 Rate of increasing data volume;
 - 11.1.4 Cost of data backup procedures and tools vs. cost if restored without backup;
 - 11.1.5 Importance of data;
 - 11.1.6 Life and reliability of data media;
 - 11.1.7 Retention schedules; and
 - 11.1.8 Confidentiality and integrity.
- 11.2 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.

12. DATA BACKUP OWNER

- 12.1 The SWDM should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, so to ensure segregation of duties and responsibilities and to mitigate the risk of systems and data losses.
- 12.2 The ICT Manager has the discretion in collaboration with the CFO, to assign ICT staff members to ensure each backup schedule is maintained. (To be implemented when disaster recovery site has been established)

13. OFFSITE STORAGE SITE

(To be implemented once a site is established)

- 13.1 Data backups must be stored in two locations:
 - 13.1.1 One on-site, or in close proximity, with current data in a machine-readable format in the event that operating data is lost, damaged or corrupted; and
 - 13.1.2 An off-site location, to additionally provide protection against loss to the primary site and on-site data.
- 13.2 Off-site backups must be a minimum of 6 kilometres from the on-site storage area to prevent a single destructive event from destroying all copies of the data.
- 13.3 Should high availability be required, additional backup copies may be securely stored in the close proximity to the ICT system (within the data centre or secure vault).
- 13.4 Minimum requirements are to store the monthly and/or yearly backup sets off-site.
- 13.5 The site used for storing data media off-site must be physically secure and safe.
- 13.6 Receipts of media being collected and delivered must be kept for record-keeping purposes and must be signed by ICT personnel in attendance.
- 13.7 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 applicable retention period.
- 13.8 All data media used to store information must be disposed of in a manner that ensures the data is not recoverable.
- 13.9 This will be implemented once an off-site storage site has been identified.

14. TRANSPORT MODES

- 14.1 When choosing the transport mode for the data (logical or physical), it is important to consider the following:
- 14.1.1 Time constraints;
 - 14.1.2 Capacity requirements; and
 - 14.1.3 Security and encryption.

15. RETENTION CONSIDERATION

- 15.1 Data should be retained in line with current legislative requirements, as defined in sections 19 and 20 of this document.
- 15.2 The minimum retention of backups is as follows:
- 15.2.1 A full system backup will be performed weekly, where possible or not longer than two (2) weeks. Weekly backups must be saved for a full month.
 - 15.2.2 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.
 - 15.2.3 Monthly backups must be saved for one year, at which time the media will be reused or disposed of.
 - 15.2.4 Yearly backups must be retained for five (5) consecutive financial years and will only be run once a year at a predetermined date and time.
 - 15.2.5 Differential or Incremental backups will be performed daily. The retention of Daily backups should be determined by the ICT Manager. Daily backup media will be reused once this period ends.

16. RECOVERY OF BACKUP DATA

- 16.1 Backup documentation must be maintained, reviewed and updated by the ICT Manager periodically to account for new technology, business changes,

and migration of applications to alternative platforms. This includes, but is not limited to:

16.1.1 Identification of critical data and programs; and

16.1.2 Documentation and support items necessary to perform essential tasks during a recovery process.

16.2 Documentation of the restoration process must include:

16.2.1 Procedures for the recovery

16.2.2 Provision for key management should the data be encrypted.

16.3 Recovery procedures must be tested at least quarterly and Disaster Recovery procedures must be tested at least yearly.

16.4 Recovery tests must be documented and submitted to the CFO and ICTCOM.

17. BACKUPS IN RECORD MANAGEMENT

17.1 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 SWDM functions, activities and transactions. The detail of these requirements can be found in:

17.1.1 The National Archives and Records Service of South Africa Regulations; and

17.1.2 Other applicable municipal policies, may include policies relating to Records Management, Employee Information, Internet and E-mail Usage, Web Content Management, Social Media Content and Document Imaging/Management in the Municipality.

17.2 The Records Manager is responsible for the implementation of sound records management principles and records disposal schedules for the SWDM. The

Records Manager is also responsible for maintaining the retention periods indicated on the file plan and disposal schedule.

- 17.3 The ICT Manager must liaise and work closely with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.
- 17.4 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. Archiving solutions may be considered for electronic records and email retention.
- 17.5 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.
- 17.6 The ICT Services Division 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:
 - 17.6.1 Backups must be made daily, weekly and monthly;
 - 17.6.2 Backups must cover all data, metadata, audit trail data, operating systems and application software;
 - 17.6.3 Backups must be stored in a secure off-site environment and no backup and backup system must be stored or hosted outside the borders of the Republic of South Africa.
 - 17.6.4 Public records being backed up must conform to the municipal File Plan;
 - 17.6.5 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.
 - 17.6.6 The backup and retrieval software/system must also be protected to be available in the event of a disaster;

-
- 17.6.7 The integrity of backups must be tested using backup test restores and media testing.
- 17.7 The ICT Manager must implement measures to ensure that systems prevent the deletion of electronic records or e-mails.
- 17.8 The ICT Manager in consultation with the 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.
- 17.9 Officials are responsible for filing e-mails. It is the discretion and responsibility of the sender or receiver to file e-mails.
- 17.10 The Records Manager, in conjunction with the ICT Manager, must create awareness among Officials of the importance of e-mail as public records. This could include, but is not limited to:
- 17.10.1 E-mails must be properly contextualised and meaningful over time;
 - 17.10.2 Subject lines are very important and must be descriptive;
 - 17.10.3 Auto-signatures must be used and shall contain full details of the sender; and
 - 17.10.4 Attachments must be filed into the file plan in the document management system before it is attached to the e-mail.
- 17.11 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.
- 17.12 The ICT Manager and Records Manager may dispose of any electronic records and e-mails if retention is not required under any Act or General Disposal Authority.

18. GENERAL RULES FOR RETENTION PERIODS

- 18.1 The National Archives provides the primary considerations when defining retention periods of electronic records and e-mails.
- 18.2 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.

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.2.1	National Archives and Record Service of South Africa Act, Act No. 43 of 1996	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 has been obtained from the National Archivist or a Standing Disposal Authority has been issued by the National Archivist against records classified against the file plan.
Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.2.2	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.
18.2.3	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.
18.2.4	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.

18.2.5	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: • 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.
--------	---	---	---

18.3 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.

18.4 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 in National Archivist legislation, regulations and guidance.

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

18.4.2	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
18.4.3	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
18.4.4	Treasury Regulations, Regulation 17	Supplementary accounting records, including, for example, cash register strips, bank statements and timesheets.	5 Years
18.4.5	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

18.5 Per the 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.

18.6 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:

18.6.1 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.

18.6.2 The original form may have reasonable validations added, which is required in the normal course of information systems communication, storage or display.

18.7 The Electronic Communication and Transaction Act, No 25 of 2005 regulates the storage of personal information:

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.7.1	Electronic Communication and Transaction Act, No 25 of 2005	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information.	As long as the information is used, and at least 1 year thereafter.
18.7.2	Electronic Communication and Transaction Act, No 25 of 2005	A record of any third party to whom the information was disclosed must be kept for as long as the information is used.	As long as the information is used and at least 1 year thereafter.
18.7.3	Electronic Communication and Transaction Act, No 25 of 2005	All personal data which has become obsolete.	Destroy

18.8 The Protection of Personal Information Act, No. 4 of 2013 ("POPI") regulates the retention of personal information:

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.8.1	Sections 9 to 18	Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views,	Do not collect or retain unless the person has been given notice and express consent is obtained. Exceptions apply. Personal information may not be

		preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears next to other personal information or if the name itself would reveal personal information about the person.	retained for longer than agreed with the person unless the retention of the record is required by law. (This principle applies to all items in this table. The retention of items that follow is expressly prohibited unless exceptions apply.)
18.8.2	Sections 6, 34 to 37	Children's information	Destroy unless exceptions apply e.g. establishment or protection of a right of the child.
18.8.3	Sections 6 & 28	Religious or philosophical beliefs	Destroy unless exceptions apply e.g. to protect the spiritual welfare of a community.
18.8.4	Sections 6 & 29	Race or ethnic origin	Destroy unless exceptions apply e.g. protection from unfair discrimination or promoting the advancement of persons.
18.8.5	Sections 6 & 30	Trade union membership	Destroy unless exceptions apply e.g. to achieve the aims of trade union that the person belongs to.
18.8.6	Sections 6 & 31	Political persuasion	Destroy unless exceptions apply e.g. to achieve the aims of a political institution that the person belongs to.
18.8.7	Sections 6 & 32	Health or sex life	Destroy unless, exceptions apply e.g. provision of healthcare services, special support for pupils in schools, childcare or support for workers.
18.8.8	Sections 6 & 33	Criminal behaviour or biometric information	Destroy unless exceptions apply e.g. necessary for law enforcement.

19. BACKUP STRATEGY

19.1 The below table is used to guide on the backup strategy. Any deviations from the strategy must be reported by the ICT Manager to the CFO.

19.2 A register of backups taken in line with the below table must be kept by the ICT Manager and be submitted monthly to the CFO and quarterly to the ICTCOM.

Data Set	Full Backup			Differential Backup	Incremental Backup
	Monthly	Weekly	Yearly	Daily	Daily

Financial Systems	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
HR Systems (Payroll, T&A, Leave, etc.)	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
File and Print Services	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
Business Enablers (Mail, eDirectory, AD, SQL, etc.)	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
Supporting Material (Application installation files)	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday

20. BACKUP DESIGN PRINCIPLES

20.1 The Municipality will need to standardise its backup solution and backup medium(s) across all sites to implement the policy. The backup medium(s) may include data replication to another site.

20.2 The following design principles and requirements have been taken into consideration in informing the Backup Architecture Design inclusive of with integrated application awareness, and is in response to several business requirements, legal constraints and technical issues:

20.2.1 Provide a unified and integrated data management solution to protect the production systems at all pertinent municipal sites and data centres;

20.2.2 Protection of the Directory and Domain Controllers;

20.2.3 Protect File Servers data on Physical Servers;

- 20.2.4 Protection of the Email Server;
- 20.2.5 Protection of the MSSQL;
- 20.2.6 Protection of the SharePoint Data;
- 20.2.7 Protection of Virtual Machines hosted on VMWare (VMware backups to be made via SANMode and Live sync to be used for Critical Virtual Servers, when required);
- 20.2.8 Maintain copies of backup data on disk or USB drive. (SAMRAS);
- 20.2.9 Maintain warm Virtual Machine warm disaster recovery site (To be implemented when disaster recovery site is established);
- 20.2.10 All Backup Clients will be protected by local media agents at Head Office and the DR site with the Disk Library in combination with deduplication. (To be implemented when disaster recovery site is established);

21. SYSTEMS PROTECTION STRATEGY

21.1 Windows File System

- 21.1.1 Windows File System Agent will be used to protect File System & System State data on local disks of Physical Servers.
- 21.1.2 Weekly Synthetic Full and Daily Incremental backup schedules will be implemented. Paths & Shares to be protected will be specified.

File System Protection:	Physical Servers (Windows File System)
Data Protection Summary	▪ Daily deduplicated Inc backup ▪ Weekly Synthetic(DASH) Full
Service Account Requirements (Permissions / Rights)	▪ Local Administrator ▪ Read\Write Access to Shared Folders

21.2 Unix/Linux File System & NFS

21.2.1 Unix/Linux File System Agent will be used to protect File System & System State data on local disks of Physical Servers.

21.2.2 Weekly Synthetic Full and Daily Incremental backup schedules will be implemented. Paths & Shares to be protected will be specified.

File System Protection:	Physical Servers (Unix\Linux File System)
Data Protection Summary	- Daily deduplicated Inc backup - Weekly Synthetic(DASH) Full
Service Account Requirements (Permissions / Rights)	- Local Administrator - Read\Write Access to Shared Folders

21.3 Active Directory and eDirectory

21.3.1 The Microsoft Active Directory Domain of SWDM is hosted on a Domain Controller. Domain Controllers are Virtual Machines in VMWare environment and Domain Controller is hosted at the Swellendam Data Site.

File System Protection:	Domain Controller
Data Protection Summary	Daily Full with Active Directory Agent

21.4 Microsoft SQL Server

21.4.1 The SWDM has MSSQL Servers, which are both Standalone MSSQL Servers and host instances & databases. The Backup Schedule will include a Daily Incremental and Transaction Log backup daily for all MSSQL Instances.

File System Protection:	MSSQL Databases
Data Protection Summary	- Daily Incremental Backup - Transaction Log Backup daily

Service Account Requirements (Permissions / Rights)	• Local Administrator • SQL Admin • System Account
--	--

21.5 VMWare Infrastructure

21.5.1 The SWDM has VMWare ESX hosts in cluster configuration in the Swellendam domain, managed by a single vCenter server per site, which needs to be protected with Virtual Server Agents. All the VMs are to be protected with VM Level backup.

VMWare Protection:	VM Guests utilising VHD-based disks(VM Level backups)
Data Protection Summary	• Daily deduplicated Incremental backup • Weekly DASH Full
VMWare Requirements (Permissions / Rights)	User accounts for • Local Administrator • VMWare Administrator role

22. **BREACH OF THIS POLICY**

22.1 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 must be reported to the Director of Financial Services which will assess its level of severity. Appropriate disciplinary action or punitive recourse may be instituted against any user who contravenes this policy.

22.2 Actions may include, but are not limited to:

22.2.1 Revocation of access to Municipal systems and ICT services;

- 22.2.2 Disciplinary action in accordance with the SWDM disciplinary procedures;
- 22.2.3 Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or
- 22.2.4 Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

23. POLICY REVIEW

- 23.1 The policy shall be reviewed annually by the ICT Steering Committee.