# Overstrand Municipality

Information, Communication and Technology

# Data Backup and Recovery Policy

*Approved by Council*

*28 March 2018*

**Abstract**

This document outlines the Data Backup and Recovery Policy within ICT covering all its core Systems, Servers and Applications within the Overstrand Municipality

## TABLE OF CONTENTS

## 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. |
| Battle box | A battle box is comprised of all the required software and detailed documented information per application, server or data set on how to recover the service in the case of a disaster at the main site. |
| 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 etc. |
| 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, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

The Backup procedure responsible for ensuring that all municipality data stored on approved systems within the Overstrand Municipality environment is recoverable in the event of accidental loss or damage.

## 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, Act No. 108 of 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. 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.

## 5. SCOPE

This policy repeals any previous ICT Backup and Disaster Recovery policies.

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. Municipalities must develop their own Data Backup and Recovery controls and procedures by adopting the principles and practices put forward in this policy.

## 6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein may be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract may be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse may 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 disciplinary procedures; 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 Manager, Systems Development is responsible for maintaining and ensuring compliance to this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and where applicable, changes approved by the Council.

## 8. DATA BACKUP STANDARDS

8.1 Critical data, which is critical to the Municipality, must be defined by the Business in consultation with ICT and must be backed up.

8.2 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 schedule.

8.3 Data restores must at least be tested quarterly.

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

(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 procedure of backed up data.

## 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, 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 be subject to the review of the ICT DR Business Impact and Risk Analysis requirements are updated with input from System Administrators, 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, 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.

10.4 For clarification purposes the ICT division may create a summary of backup types, along with their advantages, disadvantages and frequency and attach it to this policy as Annexure D.

## 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.

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 Manager, Systems Development should determine the quantity of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location.

(b) 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.

## 12. DATA BACKUP PROCEDURES

12.1 The Manager, Systems Development have the discretion to 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 or manual process of transporting backup media. | 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.<br><br>Higher risk of backup media loss or integrity.<br><br>Requires more resources to be effective. |
| Automatic Backups | Triggered by a program at certain intervals. Entire process is electronic with no manual operations required. | The backup schedule is not dependent on the discipline and reliability of an operator.<br><br>Lower risk of backup loss or media integrity.<br><br>Less resources required. | There is a cost associated with automation.<br><br>The schedule needs to be monitored and revised to include any non-standard updates and/or changes to the work schedule. |

**Figure 1 :** Advantages and disadvantages of manual and automated backups

12.2 The Manager, Systems Development have the discretion to 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, where possible, carried out on a central ICT Backup system. | Allows for more economical usage of data media. | There is added exposure to confidential data.<br><br>Confidential and non-confidential information may be combined requiring more stringent security controls for handling the backups. |
| Decentralized Backups | Performed by ICT end-users or system administrators and may or may not be transferred to a central ICT system. | ICT users can control the information flow especially in the case of confidential data. | The consistency of data backup depends on the reliability and skill level of the end-user.<br><br>High risk of data exposure or loss. |

**Figure 2 :** Advantages and disadvantages of centralized and decentralized backup procedures

## 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.

## 14. DATA BACKUP OWNER

14.1 The Municipality should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, so to ensure a segregation of duties and responsibilities and to mitigate the risk of systems and data losses.

14.2 The Manager, Systems Development has the discretion to assign at least two ICT staff members (One primary, one secondary) to ensure each backup schedule is maintained.

## 15. OFFSITE STORAGE SITE

15.1 Data backups must be stored in two locations:

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

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

15.2 Off-site backups must be a minimum of 5 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 may be securely stored in the close proximity of the ICT system (within the data centre or secure vault).

15.4 Minimum requirements are to store the monthly and/or yearly backup sets off site.

15.5 The site used for storing data media off-site must be physically secure and safe.

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

15.7 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.

15.8 All data media used to store 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 The minimum retention of backups are as follows:

(a) 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.

(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 must be saved for one year, at which time the media will be reused or disposed of.

(d) 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.

(e) Differential or Incremental backups will be performed daily. The retention of Daily backups should be determined by the ICT Staff. 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 by the Manager, Systems Development 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 quarterly and Disaster Recovery procedures must be tested at least yearly.

18.4 Recovery tests must be documented and submitted to the Manager, Systems Development.

## 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. The detail of these requirements can be found in:

(a) The National Archives and Records Service of South Africa Regulations; and

(b) Other applicable municipal policies, which 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.

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 Manager, Systems Development 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.

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. Archiving solutions may be considered for electronic records and email retention.

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 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:

(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 and no backup and backup system must be stored or hosted outside the borders of the Republic of South Africa.

(d) Public records being backed up must conform to the municipal File Plan;

(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/system must also be protected to be available in the event of a disaster;

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

19.7 The Manager, Systems Development must implement measures to ensure that systems prevent the deletion of electronic records or e-mails.

19.8 The Manager, Systems Development, 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.

19.9 Officials are responsible for filing e-mails. It is the discretion and responsibility of the sender or receiver to file e-mails. The figures below can be used as a guideline to assists with determining responsibility for retaining e-mail messages.

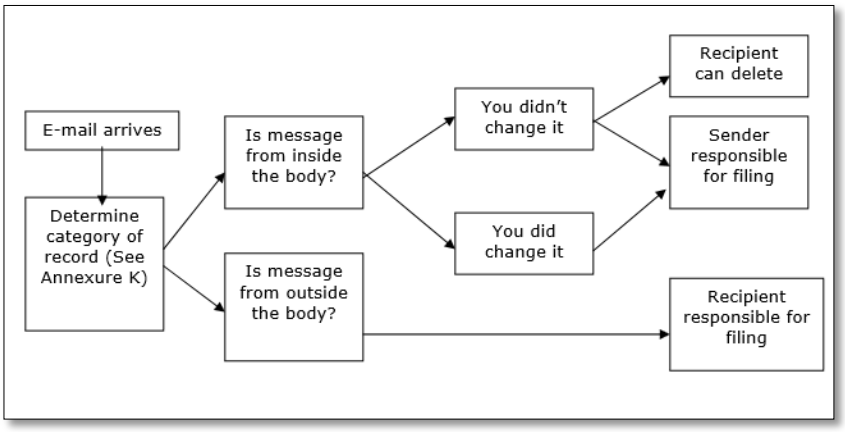


**Figure 3** : Example decision sequence to assist with determining responsibility for retaining e-mail messages (*Source: National Archives. Managing electronic records in governmental bodies: Policy, principles and requirements National Archives*)

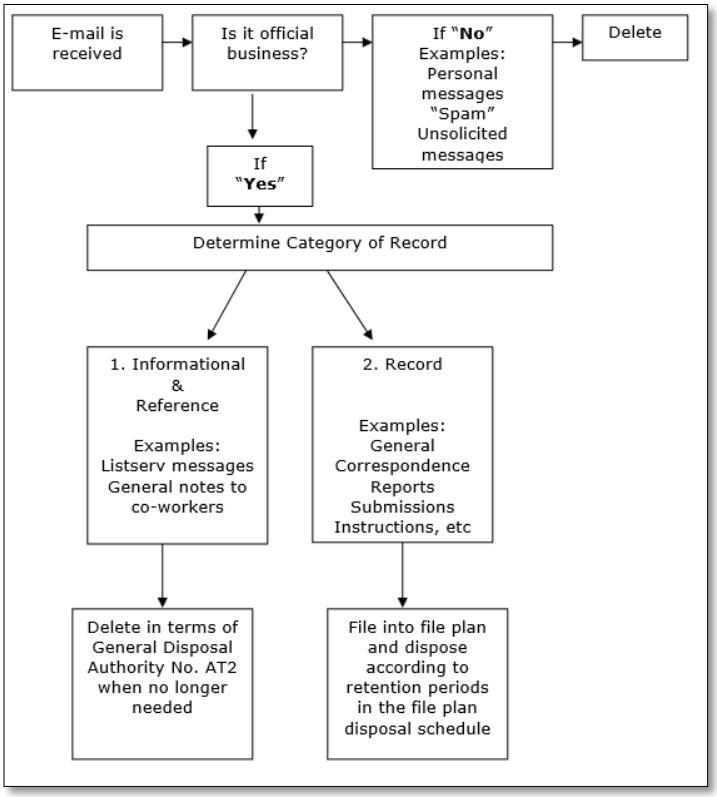


**Figure 4 :** Examples of a decision sequence for determining e-mail retention (*Source: National Archives. Managing electronic records in governmental bodies: Policy, principles and requirements National Archives*)

19.10 The Records Manager, in conjunction with the Manager, Systems Development, must create awareness with Officials of the importance of e-mail as public records. This could 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) Auto-signatures must be used and shall contain full details of the sender; and

(d) Attachments must be filed into the file plan in the document management system before it is attached to the e-mail.

19.11 The Manager, Systems Development 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.

19.12 The Manager, Systems Development and 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 support 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<br><br>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. |

| Act or National Archive Regulations and Guidance | Item | Retention period |
|---|---|---|
| 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. |
| Managing electronic records in governmental bodies Policy, principles and requirements<br><br>Managing electronic records in governmental bodies Metadata requirements | E-mails, and attachments therein, must be retained if they:<br>• Are evidence of Municipal transactions;<br>• Approve an action, authorize an action, contain guidance, advice or direction;<br>• Relate to projects and activities being undertaken, and external stakeholders;<br>• Represent formal business communication between staff; or<br>• Contain policy decisions. | E-mails fall into one of the 4 categories above and must be retained as such. |

**Figure 5 :** Retention periods specified by the National Archives

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 Municipal 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 |
| 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 |

**Figure 6 :** Retention periods specified by Treasury Regulations, Regulation 17 (guidance only)

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:

| Act | Item | Retention period |
|---|---|---|
| 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 information is used, and at least 1 year thereafter. |
| 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. |
| Electronic Communication and Transaction Act, No 25 of 2005 | All personal data which has become obsolete. | Destroy |

**Figure 7 :** Retention periods specified by the Electronic Communication and Transaction Act, No 25 of 2005

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

| Sections | Item | Retention period |
|---|---|---|
| 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, 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. | Do not collect or retain unless the person have been given notice and express consent is obtained. Exceptions apply.<br><br>Personal information may not be retained for longer than agreed with the person, unless the retention of the record is required by a law.<br><br>(This principle is applicable to all items in this table. The retention of items that follow is expressly prohibited unless exceptions apply.) |
| Sections 6, 34 to 37 | Children's information | Destroy unless, exceptions apply e.g. establishment or protection of a right of the child. |
| Sections 6 & 28 | Religious or philosophical beliefs | Destroy unless, exceptions apply e.g. to protect the spiritual welfare of a community. |
| Sections 6 & 29 | Race or ethnic origin | Destroy unless, exceptions apply e.g. protection from unfair discrimination or promoting the advancement of persons. |

| Sections | Item | Retention period |
|---|---|---|
| Sections 6 & 30 | Trade union membership | Destroy unless, exceptions apply e.g. to achieve the aims of trade union that the person belongs to. |
| Sections 6 & 31 | Political persuasion | Destroy unless, exceptions apply e.g. to achieve the aims of a political institution that the person belongs to. |
| 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. |
| Sections 6 & 33 | Criminal behaviour or biometric information | Destroy unless, exceptions apply e.g. necessary for law enforcement. |

**Figure 8 :** Retention periods specified by the Protection of Personal Information Act, No. 4 of 2013

## 21. ANNEXURE A: BACKUP TYPES

| Type | Detail | Advantages | Disadvantages | Frequency |
|---|---|---|---|---|
| Full data backup | All data requiring backup is stored on an additional data medium without considering whether the files have been changed since the last backup. | Simple and quick restoration of data due to the fact that all relevant and necessary files can be extracted from the latest full data backup. | Requires a high storage capacity.<br><br>If full data backups are not carried out regularly, extensive changes to a file can result in major updating requirements. | 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. During restoration, the latest full backup is restored first, after which incremental backups are restored to the most current state of the backed-up data. | Saves storage capacity and shortens the time required for the data backup. | Restoration time for data is generally high, as the relevant files must be extracted from backups made at different stages. | Daily. |
| Differential data backup | This procedure stores only the files that has been changed since the last full data backup. During restoration, the latest full backup is restored first, after which differential backups are restored to the most current state of the backed-up data. | Files can be restored quicker and easier then incremental backups. | Requires more capacity on the backup medium than an incremental backups. | Daily. |
| Image backup | This procedure backs up the physical sectors of the hard disk rather than the individual files on it. | Full backup which allows for very quick restoration of hard disks of the same type.<br><br>Very effective for disaster recovery. | Not useful for restoration of individual files. | Used for systems with very specific and specialized configuration. |

**Figure 9:** Advantages and disadvantages of backup types

## 22. ANNEXURE B: BACKUP STRATEGY

The below strategy is used as a guideline, alternatively the Manager, Systems Development can revise the strategy that must be strictly adhered to:

| 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 | Weekend after Financial Year end | Monday to Friday | |
| HR Systems (Payroll, T&A, Leave, etc.) | Last weekend in the month | Last day of the week | Weekend after Financial Year end | Monday to Friday | |
| File and Print Services | Last weekend in the month | Last day of the week | 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 | Weekend after Financial Year end | Monday to Friday | |
| Supporting Material (Application installation files) | Last weekend in the month | Last day of the week | Weekend after Financial Year end | Monday to Friday | |

**Figure 10:** Backup strategy

## 23. ANNEXURE C: ROLES AND RESPONSIBILITIES

| Backup Component | Responsible | Accountable | Contribute | Inform |
|---|---|---|---|---|
| Data Criticality “Rating” | ICT Application Team | ICT Application Team | ICT Team | ICT Backup Operator |
| Detailed Application/Server Build Documentation | ICT Application Team | ICT Team | ICT Backup Operator | ICT Backup Operator |
| Data Backup Selection List | ICT Team | ICT Application Team | ICT Backup Operator | ICT Backup Operator |
| Backup Monitoring | ICT Backup Operator | ICT Backup Operator | ICT Team | ICT Application Team |
| Backup Reporting | ICT Backup Operator, System | ICT Backup Operator | ICT Team | ICT Application Team |
| Media management | ICT Backup Operator | ICT Backup Operator | ICT Team | ICT Application Team |
| Offsite Storage | Offsite Data Custodians | ICT Backup Operator | ICT Team | ICT Application Team |

**Figure 11:** Roles and responsibilities

## 24. ANNEXURE D: DESIGN PRINCIPLES

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.

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 a number of business requirements, legal constraints and technical issues;

- Provide a unified and integrated data management solution protect the production systems at all pertinent municipal sites and data centres
- Protection of the Directory and Domain Controllers
- Protect File Servers data on Physical Servers
- Protection of the Email Server (MicroFocus GroupWise)
- Protection of the MSSQL
- Protection of the SharePoint Data
- Protection of Virtual Machines hosted on VMWare (VMware backups to be made via SAN Mode and Live sync to be used for Critical Virtual Servers, when required)
- Maintain copies of backup data on Disk
- Maintain warm Virtual Machine warm disaster recovery site
- 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. A copy needs be sent to Tape.

## 25. ANNEXURE E: SYSTEMS BACKUP

### 25.1 Data Retention

During the Assessment and Design session, the following Data Retention requirements have been outlined:

- All backups will be targeted to Disk and a copy of the data will be maintained on Disk and Tape at DR for short-term and long-term retention respectively.
- As per the best practices and upon reviewing the data retention requirements, data retention requirements are outlined in the table below;

| Job Type | Retention on Disk | Retention Offsite / at DR |
|---|---|---|
| All Incremental Backups | 15 Days | 15 Days Disk |
| Daily Full Backups (All Databases) | 15 Days | 15 Days Disk |
| Weekly Full Backups (All Non-Databases) | 15 Days | 90 Days Disk |
| Monthly Full | 365 Days | Tape |
| Yearly Full | 1825 Days | Tape |

**Figure 12:** Data Retention

To summarize all the backups will be performed to Disk as primary target and retained for a period of 15 Days on Premises. A Synchronous copy of all backups will be maintained on disk at the DR Site for 15 Days along with separate copy of Weekly Full on Tape for 90 Days and extended retention for Monthly Full on Tape forever. Yearly Copies to be decided by Overstrand.

Sufficient disk space will be required to achieve the Retention on Disk requirements at a growth rate of 30% per annum.

### 25.2 Key Business Processes

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for Full Disaster Recovery for Core Systems is a fully mirrored recovery site at the company's offices in Onrus.

This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site Hermanus and the backup site and backups for the recovery of single or multiple systems at the main site.

| Core System | | DR Services |
|---|---|---|
| **Type** | **Name** | |
| Works Order Systems | EMIS | Daily, Fully, mirrored recovery site |
| Messaging | GroupWise Messaging and Post Offices / Agents | Daily, Fully, mirrored recovery site |
| Financial Systems | SAMRAS/SAMRAS (Classic, mSCOA), including Web Services | Daily, Fully, mirrored recovery site for the MSSQL and Front-End Services. Refer To SAMRAS documentation for SAMRAS Classic backup schedule. |
| HR, Collaboration, Correspondence | Collaborator<br>(including SharePoint / Web Services / Front End Services) | Daily, Fully, mirrored recovery site |
| Payroll and ESS (Employee Self Service) | Payday | Daily, Fully, mirrored recovery site |
| Time & Attendance | Kronos T&A | Daily, Fully, mirrored recovery site |
| GIS | ESRI GIS | Daily, Fully, mirrored recovery site |
| MicroFocus Application Services | (Novell / MicroFocus)<br>e.g. Filr | Daily, Fully, mirrored recovery site |
| Windows, Unix\Linux File System & NFS | *NIX/NFS: Novell / MicroFocus OES<br>Windows: Microsoft Servers | Daily, Fully, mirrored recovery site |
| AD / E-Directory | E-Directory: Novell / MicroFocus<br>AD: Microsoft | Daily, Fully, mirrored recovery site |
| Database | MS SQL | Daily, Fully, mirrored recovery site |
| Virtual Infrastructure | VMWare, VMVCenter | Daily, Fully, mirrored recovery site |

**Figure 13:** Core Business Systems

| | |
|---|---|
| **System being backed up** | Data Classification: Business critical data |
| **Backup Selection** | The data required to be backed up is determined and identified by the owner of the data set on this server. |
| **Media used** | Local Disk Backup,<br>Offsite DR Backup Disks<br>Tape library with LTO 6 tapes<br>No data encryption enabled |
| **Backup Schedule** | Daily backups: Runs Monday – Friday from 18:00 – 23:00<br>Weekly backups: Runs every Saturday from 18:00 – 23:00<br>Monthly backups: Runs on the last Saturday of the month from 18:00 – 23:00 and replaces the Weekly backup for this scheduled period.<br>Yearly backup: Is manually run after financial yearend |

| | |
|---|---|
| **Data Retention** | Daily backups: Media set is retained for 2 weeks<br>Weekly backups: Media set is retained for 1 month<br>Monthly backup: Media set is retained for 1 year<br>Yearly backup: Media set is retained for 5 years |
| **Offsite Storage** | All media is moved and stored offsite at a secured facility after the successful completion of the backup.<br>The same facilitator providing the offsite storage, is used to provide transport of the media to the secure site. |
| **Data Backup Owner** | The Tape backup is monitored and media is inserted on a daily basis by the backup administrator. |

## 26. ANNEXURE F: TAPE BACKUP ROTATION

26.1 **Overstrand IT is responsible for:**

1. Changing tapes: Once a month the disk backups are migrated to tape. These tapes are then removed and taken offsite and new tapes added to the library. IT must ensure that these migrations have taken place and logs must be kept of these migrations.
2. The backup tapes are stored offsite at the Onrus DR Site
3. All backup notifications are sent to three support personal, two Overstrand Administrators and Lateral Dynamics to ensure the success of the backups and the recovery of any failures.

26.2 **Verification of Backup Status**

Every morning, the backup notifications are verified by the ADMINISTRATOR: IT.

26.3 **Backup Log**

A daily backup log is issued (emailed) to keep a report of backups, their status, which tapes are used and housekeeping of the backup system. These logs are stored within the Backup System and Administrator email.

26.4 **House-keeping of the Backup System**

Regular maintenance of the backup device is carried out to ensure it is kept in good working order. Cleaning tapes are used in accordance with manufacturer's instructions. DLT tape drives should be cleaned monthly.

26.5 **Managing Backup Failure**

In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:

4. Note any messages / information in the log file
5. Contact the senior IT Officer and Manager to report the failure
6. Record the failure in the backup log and any actions taken as a result
7. Restart the backup or ensure that the cause of failure is solved before next backup schedule (if this is a viable course of action). If not, the affected business unit or department will be informed and a new course of action will be mutually agreed.
8. If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time, and must be performed when all users are logged out. This will include logging the call with the Backup Vendor to identify the underlying cause and report back to management.

## 26.6 Storage of Backup Tapes

The backup tapes, when removed from the server, are stored securely in an off-site secure location (locked fire-proof safe).

At any time there should be:

- Two or more complete backups, 7 days old stored, at the Hermanus Data Centre premises
- Two or more complete backup tapes, 30 days old stored, off-site at a secure location.

## 26.7 Validation of Backup Tapes

A backup tape is validated by the Support Officer: ICT every 3 months. As part of this process the Support Officer: ICT will check to ensure data can be fully restored from the tape.

## 26.8 Management of Tapes

Backup Volumes are clearly labelled with a month or server and used in strict rotation to ensure even wear and immediate identification of any problems with a specific tape.

## 27. ANNEXURE G: SYSTEMS PROTECTION STRATEGY

### 27.1 Windows File System

Windows File System Agent will be used to protect File System & System State data on local disks of Physical Servers.

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

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

### 27.2 Unix\Linux File System & NFS

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

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

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

### 27.3 Active Directory and eDirectory

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

The MicroFocus E-Directory for the Overstrand are hosted on various UNIX machines as a Federated Directory Service. E-Directory Controllers are Virtual Machines in VMWare environment hosted at the Hermanus Data Site as well as at each Administration for fault tolerance.

| | |
|---|---|
| **File System Protection:** | Domain Controller |
| **Data Protection Summary:** | • Daily Full with Active Directory Agent |

## 27.4 Microsoft SQL Server

The Overstrand has MSSQL Servers, which are both Standalone MSSQL Servers and host instances & databases. Backup Schedule will include a Daily Full and Transaction Log backup every 6 hours for all MSSQL Instances.

| | |
|---|---|
| **File System Protection:** | MSSQL Databases |
| **Data Protection Summary:** | • Daily Full Backup<br>• Transaction Log Backup every 1Hr |
| **Service Account Requirements (Permissions / Rights)** | • Local Administrator<br>• SQL Admin<br>• System Account |

## 27.5 Microsoft SharePoint Server

The Overstrand environment consists of SharePoint Server(s) in Production and Development environments; with a mix of Web App Servers and Front-End Servers.

The Overstrand will utilise a Microsoft SharePoint Agent on the SharePoint Application Servers in Production environment to enable granular backup & recovery of Site Collections and Documents, VM Level Backup will also be configured for the SharePoint servers to provide full system recovery capabilities. SharePoint Databases are hosted on MSSQL database which will be protected with an MSSQL Agent.

The database or farm level backup protects all databases within the SharePoint environment as well as IIS configuration and customisations residing as files on the Windows file system.

| SharePoint Data | Data Protection Summary |
|---|---|
| Application | • Weekly DASH Full & Daily Incremental backup |
| SharePoint Databases | • Backup using the SQL Agent installed on the SQL 2014 SQL client.<br>• Daily Full<br>• TLog backup every 6hrs |
| Web & App Servers | • Weekly DASH Full & Daily Incremental Backup |

| | |
|---|---|
| **Service Account Requirements (Permissions / Rights)** | • A Windows AD domain user account with the following account privileges:<br>• Local administrative rights (Part of local Administrators group)<br>• FARM administrator rights<br>• Full permission to additional settings (registry key)<br>• SP Shell administrator permissions<br>• Full control under Policy for Web Application for |

| | |
|---|---|
| | every Web Application<br>• SQL System Admin Server Role for the instance where SharePoint Databases resides<br>• Site Administrator permissions for all Site Collections<br>• Full permissions to the Job Results and Log Files folders |
| **SQL server Services account for SharePoint instance.**<br>**SharePoint Services Timer Account**<br>**All Web Application Pools Accounts** | • Full permissions to the Job Results and Log Files folders |

## 27.6 GroupWise

To secure a GroupWise database at the Overstrand Municipality, the (Unix) OES File System Agent will be used. Any other agent (e.g., Windows File System) cannot be used to secure a GroupWise database).

Clients need to be scheduled to perform weekly one full backup and daily incremental backups.

| | |
|---|---|
| **File System Protection:** | GroupWise Databases |
| **Data Protection Summary:** | • Backup using the OES Agent installed on the Servers<br>• Weekly Full & Daily Incremental Backup |
| **Novel GroupWise Requirements (Permissions / Rights)** | User account for Novell / MicroFocus SMS<br>• User account credentials to log onto the Novell SMS (Storage Management Services).<br>• User account for Target Service Agent (TSA) |

## 27.7 VMWare Infrastructure

The Overstrand Municipality has VMWare ESX hosts in cluster configuration in the Overstrand 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<br>(VM Level backups) |
| **Data Protection Summary:** | • Daily deduplicated Incremental backup<br>• Weekly DASH Full |
| **VMWare Requirements (Permissions / Rights)** | User accounts for<br>• Local Administrator<br>• VMWare Administrator role |

## 28. ANNEXURE H: 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.


| | |
|---|---|
| **POLICY SECTION:** | ICT |
| **CURRENT UPDATE:** | - |
| **PREVIOUS REVIEW:** | - |
| **APPROVAL BY COUNCIL:** | 28 MARCH 2018 |