SENQU
MUNICIPALITY

Data Backup, Recovery and Retention Policy

Date Approved	Version	Resolution Number
30 June 2016	1	10.3.2
28 July 2017	2	019/OCM/17

The Information Technology Manager

Senqu Local Municipality

19 Murray Street

Lady Grey

Telephone (051) 603 1300

Facsimile (051) 603 0445

Website: www.senqu.gov.za

Data Backup, Recovery and Retention Policy

This document sets out Senqu Municipality’s policy towards taking backups of its information assets, including their frequency, storage, retention, documentation and restoration.

Resolution: 019/OCM/17 Approved 28 July 2017

Table of Contents

1. Version Control

Full Title	**Senqu Municipality Data Backup and Recovery Policy**
Short Title	Data Backup, Recovery and Retention Policy
Author(s)	Mr R Johl
Version	0.1

Authors	Mr R Johl (PWC) & Ms. Magdalena Oertel (Senqu)
Version	01
Authorised By	Council
Authorisation Date	30 June 2016
Effective Date	1 July 2016

Revised	Ms. Magdalena Oertel (Senqu Municipality)
Version	02
Authorised By	Council
Authorisation Date	28 July 2017
Effective Date	1 July 2017

2. Definitions

Term	Meaning
IT	Information Technology
ICT	Information and Communication Technology
Municipality, the	Senqu Municipality
EC	Eastern Cape
Periodic	Containing a series of repeated functions according to time specified eg. Daily, Weekly, Monthly, Quarterly, Annually
Regularly	Containing a series of repeated functions according to time specified eg. Daily, Weekly, Monthly, Quarterly, Annually
Secure Location	Location physically different from original creation and usage location with security measures such a locked doors, logs for visitors,
Sufficient Distance	
Critical Data	Data that can severely disrupt services when lost; this data includes financial data, client personal data etc
Capacity	The amount of space utilised
Medium	Device on which data is stored eg Tapes, hard disks, CD/DVD etc

3. ICT Standards

The following are internationally recognised ICT standards were utilised in development of this policy:

- **The King III Code**: The most commonly accepted Corporate Governance Framework in South Africa is also valid for municipalities. ICT was used to inform the Governance of ICT principles and practices and to establish the relationship between Corporate Governance of and of ICT.

- **ISO/IEC 38500:** Inter nationally accepted as the standard for Corporate Governance of ICT; ICT provides governance principles and a model for the effective, efficient, and acceptable use of ICT within municipalities.

- Other: Internationally accepted process frameworks for implementing Governance of ICT.

Corporate Governance of ICT encompasses two levels of decision-making, authority and accountability to satisfy the expectations of all stakeholders. These levels are:

- Facilitating the achievement of a municipality’s strategic goals (Operational Governance of ICT); and

- The efficient and effective management of ICT service delivery (Operational Governance of ICT).

The implementation of Corporate Governance of ICT in Municipalities thus consists of the following layered approach:

- This Municipal Corporate Governance of ICT Policy, which addresses the Corporate Governance of ICT layer at a strategic level.

- Other best practice frameworks which will be adapted to give effect to the governance of the ICT operational environments within municipalities.

Corporate Governance in Municipalities:
Corporate governance is a vehicle through which value is created within a municipal context. Value means realising benefits while optimising resources and risks. This value creation takes place within a governance system that is established by the municipal policy. A governance system refers to all the means and mechanisms that enable the municipality's Council and Management team to have a structured and organised process.

Corporate Governance of the ICT in Municipalities:
The Corporate Governance of ICT is an integral part of the corporate governance system in municipalities. The Corporate Governance of ICT involves evaluating, directing and monitoring the alignment of the municipal ICT strategy with the municipal IDP's and related strategies. The Corporate Governance od ICT also involves the monitoring of ICT service delivery to ensure a culture of continuous ICT service improvements exist in the municipality. The Corporate Governance of ICT includes determining ICTICT strategic goals and plans for ICT service delivery ad determined by the Service Delivery and Budget Implementations Plan (SDBIP) objective of the municipality.

Municipal Corporate Governance of ICT Policy Objectives:

- Institutionalising a Corporate Governance of ICT Policy that is consistent with the Corporate Governance Framework of the municipality;

- Aligning the ICT strategic goals and objectives with the municipality's strategic goals and objectives;

- Ensuring that optimum Municipal value is realised from ICT-related investment, services and assets;

- Ensuring that Municipal and ICT-related risks do not exceed the municipality's risk appetite and risk tolerance;

- Ensuring that ICT -related resource needs are met in an optimal manner by providing the organisational structure, capacity and capability.

- Ensuring that the communication with stakeholders is transparent, relevant and timely; and

- Ensuring transparency of performance and conformance and driving the achievement of strategic goals through monitoring and evaluation.

4. Introduction

This policy defines the best practices to ensure reliable, accurate, acceptable backup and restoration of the systems and its associated data. It aims at standardising the backup methodologies used to improve the integrity of the hosted systems and the safekeeping of the data.

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

Computer information systems and electronic data are valuable assets to Senqu Municipality and a substantial investment in human and financial resources has been made to create the existing systems and information and, as such, a formalised policy has been implemented to:

- Address the risk of losing data
- Safeguard the confidentiality and integrity of information contained within these systems
- Ensure availability of critical data so that information can be utilised as the valuable asset that it is.
- Reduce business and legal risk.

5. Purpose

The purpose of the backup policy is to prevent the loss of data in the case of accidental deletion or corruption of data, system failure or disaster and to safeguard the information assets of Senqu Municipality by managing and securing backup and restoration processes and the media employed in the process.

6. Scope/Audience

This policy applies to all employees of the Senqu Municipality and all parties that interact with the information and systems of the Municipality. This policy covers all Information Systems environments operated by the Municipality or contracted with a third party by the Municipality.

7. General Controls

7.1 Regardless of classification, the availability of all data must be maintained by means of periodic back-ups and recovery mechanisms.

7.2 All data relating to applications, information and configuration must be backed up regularly and taken off-site to a secure location.

7.3 All data and software that is essential to the continued operation of the municipality must be backed up regularly. Refer to Appendix A for backup-Schedule.

- Ownership of all electronic information residing on any departmental computer system vests in the Municipality and Management may peruse, monitor and take copies of any information or communication made or received utilizing any of the aforementioned systems.

  - Media will not be encrypted. (Backup media and software may change and become incompatible with older encrypted backups. This complicates recovery and makes the risk of losing data due to encryption higher than the risk of media locked up in a safe and being stolen and used.)

Data to be backed up include the following:

- Users data stored on the file server in each user's allocated directory
- Exchange Server and all Emails
- Mailboxes
- System state of all servers
- Incremental, Deduplication and Universal Restore for the following servers:
  1. PDC (Primary Domain Controller)
  2. BDC (Backup Domain Controller)
  3. WSUS (Windows Update Server)
  4. MAIL SERVER (Email Server)
  5. FIN SERVER (Financial/Cloud Server)

Data Excluded

Not all files will be backed up. The following extensions will be omitted:

- Avi
- Mpeg/Mpg/Mpe
- Mkv
- Mp2
- Mp4
- Vob
- Wsf
- Wma/Wmv
- Wav

It is the responsibility of the user to back-up any data stored on the computer, laptop or an external device as this will not be backed up by the system.

7.4 Servers and systems must be backed up using the following backup methods used by Senqu Municipality:

			Incremental	**Validation Times**		
Servers	**All Hard Disks**		**Daily Times**	**Weekly Saturday**	**2nd Validation - Saturday**	**2nd Validation - Sunday**
PDC	C,D		00.00-01:00 12:00-13:00	00:00-02:00	02:30-04:30	
BDC	C		01:00-02:00 13:00-14:00	05:00-07:00	07:30-09:30	
MIS-Server	C		02:00-03:00 14:00-15:00	10:00-12:00	12:30-14:30	
EDMS	C		03:00-04:00 15:00-16:00	15:00-17:00	17:30-19:30	
Exchange	C		04:00-05:00 16:00-17:00	20:00-22:00	22:30-	00:30
SenApp	C		05:00-06:00 17:00-18:00	01:00-03:00		03:30-05:30
SebSQL	C		06:00-07:00 18:00-19:00	06:00-08:00		08:30-10:30
CW-Server	C,D		07:00-08:00 19:00-20:00	11:00-13;00		13:30-15:30
WSUS	C		08:00-09:00	16:00-		18:30-

			20:00-21:00	18:00		20:30
BackupServer	C		09:00-10:00 21:00-22:00	21:00-23:00		23:30-00:00

Backups at Senqu Municipality are Incremental and are replicated to internal and external hard disks. All backups are inclusive of all data at the municipality as well as system image files for each server.

7.5 Adequate back-up facilities must be provided to ensure that all essential business information and software could be recovered following a disaster or media failure.

7.6 An appropriate storage medium must be used. This may be disk, CD, tape, external hard drive, a mirrored server at a remote site, or any other recognised medium.

7.7 Back-up arrangements for individual systems and related data must be tested according to a formal schedule to ensure that they meet the requirements of the Municipality's Disaster Recovery Plan. Please refer to Appendix B for testing plan.

7.8 Backup media not in use any longer must be securely disposed of, rendering the data on it unreadable.

Reference to POPI:

"(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

(6) The responsible party must restrict processing of personal information if—
(a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;
(b) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;
(c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

(d) the data subject requests to transmit the personal data into another automated processing system.
(7) Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.
(8) Where processing of personal information is restricted pursuant to subsection (6), the responsible party must inform the data subject before lifting the restriction on processing."

7.9 Consideration must be given to the ability to access media in the future, in a time when technology changes, as well as the possibility of deterioration of media used for storage of records.

7.10 It is the duty of the user to ensure that all work related documents are restored on the file server under his/her allocated directory. The cost of recovery of work related data stored on a user's computer, laptop or any external device may be charged to the user.

Senqu Municipality employees have the following responsibilities:

In addition to workstations, employees have been allocated space per user, secured per user logon ID, on the File-server. The onus in on the employee to ensure that the server space allocated is utilised to the optimum.
All Business critical data on local computer and notebook hard drives must be kept, copies or moved to the specific folder allocated to the user on the file server, where it will be backed up. Where such an action is not possible, as in cases where it is done away from access to Senqu Local Municipality network, the data must be copied over on the first available opportunity. It will be the sole responsibility of the employee, under all circumstances, to backup and maintain security regarding personal data.

8. Backup and Restoration

- All applications, operating systems, data (including databases), user configuration information and hardware configuration information (where applicable) must be backed up in accordance with Appendix A.

- Appendix A determines the type of backups to be performed, the periodicity or schedule of the backup, the protection to be provided to backup media based on the criticality of the information backed up as determined by the Municipality.

- Separate systems specific backup and restoration procedures must be developed in accordance with system requirements and vendor recommendations. These procedures must be documented and implemented during and as part of system implementation.

- Users that need files restored must submit a request to the ICT Section desk by completing IT Section – Data Restore Request Form.
  Information regarding the request where possible must include the file creation date, the name of the file, the last time it was changed, and the date and time deleted or destroyed. “All requests to restore a user’s data, residing on File-servers or Exchange-servers (mail-box data), not requested by the employee or without the permission of such user, must be authorised by a Senior Manager and may be accessed by the external IT Support as per contract or any member if the IT Section.

- The IT Manager must ensure that all back-ups are successfully completed. In addition to backing up departmental data, IT Section shall perform regular disk capacity management on all data servers and have the right to delete all non-departmental related data after consultation with involved employees.

- The IT Manager must monitor the status of all backups that are performed and any faults identified must be rectified.

- The IT Manager and IT staff must ensure that a backup is made by each Senqu employee before and after installing batches or upgrades or making any configuration changes on the system. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs or other techniques.

9. Backup Frequency

8.1. The frequency of data backup for each system must be determined by considering the ‘Availability’ and ‘Integrity’ criteria as determined by the Municipality

8.2. At least three generations or cycles of back-up information must be retained for important business applications and critical data.

8.3. Additional number of generations or cycles of backup must be determined by taking into account the criticality and specific requirements of different systems.

10. Testing of Backup Media

- The IT Manager must check the quality of the backup media regularly and make sure that it is in a good condition to be re-used.

- All media on which sensitive, valuable or critical information is stored for periods longer than six (6) months must be tested at least annually to ensure that the information is still recoverable.

- After completion of backup testing, all data must be safely erased from the test environment.

11. Testing of Restoration Procedures

- The IT Manager is responsible for testing system software and data backups by restoring a sample of the backups according to a formal schedule in the test environment to ensure that it does not impact on the production environment. Refer to the formal test schedule on Appendix B.
- The IT Manager is to be responsible for controlling and supervising backup testing.

- Restoration procedures must be regularly checked at least on a monthly basis and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

- Documented evidence of the back-up restorations must be retained as per backup logs in Appendix B.

12. Backup Storage

- Backup media must be stored off-site, at an environmentally-protected and access-controlled site, at a sufficient distance to escape any damage from a disaster at the main site.

- Backup media must be stored off-site, where the possibility of the risk occurring at the site is minimal, in order to be available in the event of a disaster or for long term storage.

- Backup media that may be transported from the Server Room to the offsite storage location must be logged.

- The on-site backup media log must contain the following information:

12.4.1. Date of taking the backup
12.4.2. Date of transporting the media to the offsite storage location
12.4.3. Contents of the media (e.g. transaction backup, application backup, entire system backup)
12.4.4. Nature of backup (e.g. full image copy or file copy)

12.4.5. Name of the Carrier
12.4.6. Name of the off-site storage location
12.4.7. Name and signature of the responsible person at the onsite location
12.4.8. Any other label information

- Backup media that may be received from the Server Room and stored at the off-site storage location must be logged at the off-site storage location.

- The off-site backup media log must contain the following information:

12.6.1. Date of receiving the media at the offsite storage location
12.6.2. Contents of the media (e.g. transaction backup, application backup, entire system backup)
12.6.3. Nature of backup (e.g. full image copy or file copy)
12.6.4. Name of the Carrier
12.6.5. Name of the original location
12.6.6. Name and signature of the responsible person receiving the media at the off-site storage location
12.6.7. Any other label information

- A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, must be stored in a remote location, at a sufficient distance from the Municipality's Server Room to escape any damage from a disaster at the main site.

- At least two copies of fully recoverable versions of all critical data must be made. One copy must be stored at the Server Room whereas the other copy must be stored at an off-site storage location.

- Back-up information must be given an appropriate level of physical and environmental protection consistent with the standards applied at the Server Room.

13. Backup Retention

13.1. Backups of all data must be retained such that all systems are fully recoverable. At a minimum, yearly backup must be retained for at least 5 years.

13.2. All archival back-up data stored off-site must be reflected in an up-to-date directory which shows the date when the information was most recently modified as well as the nature of the information.

13.3. All media stored for periods longer than six (6) months must not be subject to rapid degradation.

14. Backup Documentation

14.1. Backup documentation must include identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.

14.2. Each backup media must be appropriately labelled with details of identifying criteria, date, nature of backup (e.g. Full image or incremental). In addition, it must be given a classification label, as determined by the Municipality.
The following is the minimum identifying criteria for backup media:

- Server name
- Description of the Contents
- Creation Date
- Sensitivity Classification (Based on applicable electronic record retention regulations).
- The Municipality Contact Information

14.3. Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes and migration of applications to alternative platforms.

15. Policy Violations

- Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

16. Policy

- This policy is subject to annual review or whenever it is deemed necessary by Senqu Municipality, to ensure that it is aligned to prevailing resolutions, regulations and market conditions.

17. Publishing the policy

- The policy shall be made available and accessible to all employees through soft copies via email. An electronic signature will be implemented a proof that that the policy has been received and read.

18. Senqu Municipality Approval and Sign-Off

Date of Approval by Council: 28 July 2017
Resolution Number: 019/OCM/17

________________________________ DATE ________________

MM YAWA
MUNICIPAL MANAGER

RECOMMENDATION

That the report be noted,
That the IT Data Backup Recovery and Retention Policy as part of the ICT Corporate Governance Framework be approved by Council.

Appendix A: Backup Schedule

Table 2: Backup Schedule

Back-up Schedules

Hours **Week**	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00
Servers																						
PDC	🟩										🟦											
BDC		🟩										🟦										
MIS-Server			🟩										🟦									
EDMS				🟩										🟦								
Exchange					🟩										🟦							
SenApp						🟩										🟦						
SebSQL							🟩										🟦					
CW-Server								🟩										🟦				
WSUS									🟩										🟦			
BackupServer										🟩										🟦		

Validation Schedules

	Hours **Saterday**	00:00	00:30	01:00	01:30	02:00	02:30	03:00	03:30	04:00	04:30	05:00	05:30	06:00	06:30	07:00	07:30	08:00	08:30	09:00	09:30	10:00	10:30
Servers																							
PDC		🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦												
BDC												🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦		
Exchange																						🟩	🟩
CW-Server																							
Mis-Server																							

	Hours **Sunday**	00:00	00:30	01:00	01:30	02:00	02:30	03:00	03:30	04:00	04:30	05:00	05:30	06:00	06:30	07:00	07:30	08:00	08:30	09:00	09:30	10:00	10:30
Servers																							
SenApp		🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦												
SebSQL												🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦		
EDMS																						🟩	🟩
WSUS																							
BackupServer																							

Appendix B: Backup Test Schedule

			Incremental	**Full Backup**			Backup test results
Servers	**Medium (Internal and External Hard Disks)**	**Daily**	**Daily**	**Weekly**	**Monthly**	**Yearly**	
PDC							
BDC							
MIS-Server							
EDMS							
Exchange							
SenApp							
SebSQL							
CW-Server							
WSUS							
BackupServer							