

29/10/2024

Standard Operating Procedure (SOP)

Mogale City Local Municipality
Data Ownership and Service
Provider Obligation

Standard Operating Procedure (SOP) Data Ownership and Service Provider Obligation

1. Purpose

To ensure that all municipal data created, processed, or stored by third-party service providers remains the property of the Municipality and is managed in accordance with South African legislation, information security standards, and operational requirements.

2. Applicable Legislation

- Protection of Personal Information Act (POPIA), Act 4 of 2013
- Municipal Finance Management Act (MFMA), Act 56 of 2003
- Companies Act, Act 71 of 2008
- Electronic Communications and Transactions Act (ECTA), Act 25 of 2002
- National Archives and Records Service Act, Act 43 of 1996
- Cybercrimes Act, Act 19 of 2020

3. Scope

This SOP applies to all third-party service providers contracted to develop, host, support, or maintain municipal systems, regardless of platform or location. It includes all municipal data and databases such as:

Common Relational Database Management Systems (RDBMS)

Oracle Database, Microsoft SQL Server, MySQL, PostgreSQL, IBM Db2, MariaDB, SQLite, SAP HANA, Teradata, Amazon Aurora

NoSQL and Other Database Types

MongoDB, Redis, Cassandra, Elasticsearch, Couchbase, Neo4j, Amazon DynamoDB, Google BigQuery, Firebase Realtime Database

This list is not exhaustive and includes any system storing, processing, or transmitting municipal data.

4. Roles and Responsibilities

ICT Division

- Enforce data management and security compliance
- Conduct annual compliance reviews

- Execute exit audits at contract termination

Service Providers

- Ensure data integrity, confidentiality, and availability
- Maintain compliance with POPIA, municipal ICT security policies, and industry standards
- Perform and deliver backups as required

5. SOP Steps

Step 1: Contract Initiation

- Include a data ownership clause in the SLA.
- Specify backup, encryption, data-destruction, and handover obligations.
- Identify all systems that will store, process, or transmit municipal data.

Step 2: Data Handling During the Contract

- Perform regular encrypted backups as agreed in the SLA.
- Maintain compliance with POPIA and relevant security standards (e.g., SOC 2).
- **Where a system is hosted outside of the Municipality's infrastructure, the service provider must generate monthly database/data-dump backups and submit these (in unencrypted format) to the Municipality on a quarterly basis.**
- Backups must be complete, tested, and stored securely.

Step 3: Contract Termination / Exit Procedure

- Provide a full SQL backup (or equivalent non-proprietary data-dump format).
- Deliver all necessary decryption keys, credentials, and documentation.
- Provide a signed data integrity confirmation.
- Destroy all municipal data in the provider's possession and issue a destruction certificate.

Step 4: Compliance Verification

- ICT Division conducts an exit audit to confirm:
 - Full data handover
 - Disposal certification

- Retention and access logs
- Archive all audit logs and retention reports securely.

6. POPIA Compliance Matrix

Requirement	Action	Responsible Party
Lawful Processing	Include POPIA clauses in SLA	ICT Division
Data Minimization	Limit access to only necessary data	Service Provider
Security Safeguards	Encrypt all transfers and protect backups	Service Provider
Breach Notification	Notify the Municipality within 72 hours	Service Provider

7. Risk Assessment Table

Risk	Impact	Mitigation
Unauthorized Data Access	High	Enforce encryption & access controls
Non-compliance with POPIA	High	SLA clauses, compliance reviews, audits
Data Loss During Exit	Medium	Mandatory backups, integrity checks

8. Enforcement

Service providers who fail to comply may face penalties, contract termination, and legal action under POPIA, MFMA, and the Cybercrimes Act.

9. Review

This SOP must be reviewed annually by the ICT Division in consultation with the ICT Governance Committee.

Vendor Quick Guide

Your Responsibilities:

- All municipal data remains the property of the Municipality.
- Provide a full SQL backup within 10 business days of contract termination.
- Provide all encryption keys, access credentials, and documentation.
- Destroy all municipal data after handover and provide written confirmation.
- Submit quarterly unencrypted copies of monthly database/data-dump backups for systems hosted outside the municipal infrastructure.
- Comply with POPIA and municipal ICT security policies.
- Non-compliance may result in penalties and legal action.

Compliance Checklist:

- SLA contains data ownership clause
- Full SQL backup delivered in required format
- Encryption keys and credentials provided
- Data integrity verified
- Destruction certificate received
- POPIA compliance confirmed
- Quarterly backup submissions (for externally hosted systems) verified

Compliance Audit Checklist

Audit Item	Status	Notes
SLA includes data ownership clause	☐	
Backup delivered in SQL/non-proprietary format	☐	
Quarterly backup submission received (externally hosted systems)	☐	
Encryption keys and credentials provided	☐	
Data integrity verified	☐	
Destruction certificate received	☐	
POPIA compliance confirmed	☐	

SLA Annexure Template

Annexure: Data Ownership, Backup, and POPIA Compliance

- All municipal data remains the property of the Municipality at all times.
- The service provider shall comply with POPIA and all relevant South African legislation.
- The service provider shall maintain secure, encrypted backups during the contract period.
- **For systems hosted outside the Municipality's infrastructure, the service provider must submit unencrypted copies of monthly database/data-dump backups to the Municipality on a quarterly basis.**
- Upon termination, the service provider shall:
 - Deliver a full SQL backup or equivalent non-proprietary format

- Provide all encryption keys, credentials, and documentation
 - Destroy all municipal data in its possession
 - Issue a written destruction certificate
- Breach of these obligations will result in penalties, contract termination, and possible legal action.