

**Pixley ka Seme
District Municipality**



IT Backup Policy

Table of Contents

- 1. **TERMS AND DEFINITIONS**3
- 2. **PURPOSE AND INTENTION OF THE POLICY**3
- 3. **SCOPE**.....3
- 4. **FREQUENCY OF DATA BACKUP**4
- 5. **BACKUP MEDIA**4
- 6. **RESTORING OF BACKUP DATA**.....5
- 7. **BACKUP MEDIA STORAGE LOCATION**.....5
- 8. **POLICY REVIEW**.....5

U.d

1. TERMS AND DEFINITIONS

Backup - The process of creating copies of electronic data and records and storing them on secure storage media to prevent data loss in the event of system failure, accidental deletion, corruption, or disaster.

Backup Media - Any physical or electronic device used to store backup data, including but not limited to external hard drives, tape drives, servers, cloud storage, or other approved storage technologies.

Disaster Recovery - The process of restoring data, systems, and ICT services following a disruption, disaster, or major system failure to ensure continuity of municipal operations.

Electronic Data - All data created, received, processed, or stored electronically by municipal officials and systems in the execution of official duties.

Offsite Storage - A secure storage location physically separate from the primary municipal premises, used to store backup data for protection against site-specific disasters.

Onsite Storage - A secure storage location within municipal premises where backup data is stored for quick access and recovery.

Restore - The process of retrieving backed-up data from storage media and reinstating it onto a live system, server, or workstation.

System Owner - The department or official responsible for the operation, integrity, and data generated by a specific municipal system.

2. PURPOSE AND INTENTION OF THE POLICY

The purpose of this policy is to protect municipal electronic data and records in case of accidental loss.

- To provide schedules for backing up municipal data for safekeeping.
- To ensure lost data due to forces beyond human control is restored in a reliable and up to date format.
- To provide guidelines for safeguarding and disposing of backup data.
- To protect municipal electronic data so that it can be recovered in the event of an equipment failure or intentional destruction of data.
- To regulate the backup frequencies for municipal electronic data.
- To comply with applicable legislation with regard to storing and archiving of municipal electronic records and information.

3. SCOPE

The backup policy applies to all data generated by municipal officials in pursuit of their official duties. The policy applies to all data generated from all the servers of the municipality which include, but not limited to:

- PayDay System
- Solar Financial System
- BarnOwl Internal Audit System

4. FREQUENCY OF DATA BACKUP

Backup schedules should be done as follows:

Solar Financial System

Full backups must be performed every **evening** after working hours on Mondays, Tuesdays, Wednesdays, Thursdays and Fridays of every week;

Should it not be possible to do backups on any of the stipulated days due to maintenance reasons or other unforeseen circumstances, the backups should be performed the next morning before normal knock-on time;

If it is not possible to do a backup on a Friday due to maintenance or unforeseen circumstances, the backups should be done the following Monday before users start to work on their computers;

The backup will be done automatically by the Financial system and backup data kept at the onsite as well as offsite backup server.

PayDay Systems (HR and Payroll)

Full backups must be performed on a weekly basis and backup data kept at the onsite as well as offsite backup server.

Should it not be possible to do backups on any of the stipulated days due to maintenance reasons or other unforeseen circumstances, the backups should be performed the next morning before normal knock-on time;

BarnOwl (Internal Audit Systems)

Full backups must be performed on a weekly basis and backup data kept at the onsite as well as offsite backup server.

Should it not be possible to do backups on any of the stipulated days due to maintenance reasons or other unforeseen circumstances, the backups should be performed the next morning before normal knock-on time;

5. BACKUP MEDIA

There will be a separately assigned backup folders for each backup day (i.e. Monday, Tuesday, Wednesday and Thursday OR its date equivalent i.e. dd/mm/yyyy);

Backup data shall be kept safe at an onsite as well as offsite storage location.

Backup Data for each system must be retained for a period covering the current date and extending back one full calendar month and shall be kept safe at an onsite as well as an offsite storage location/storage media.



6. RESTORING OF BACKUP DATA

Users that need files to be restored must submit a request to the IT Office.

The following information must be filled in the request form:

1. File creation date
2. The name of the file
3. The last time it was changed
4. The date and time it was deleted or destroyed.

Any possible reason for loss of data

It is the duty of municipal officials to ensure they are connected to the main network server while at work in order to ensure an updated data is recorded in the servers. Officials must take all reasonable steps to safeguard the data and media they are using to avoid frequent requests for data restore.

The backup data for Solar Financial System and backup data for other systems shall be tested on a bi-yearly(6 months) basis to ensure that the data stored/ backed up on them can be restored when needed. Furthermore, a backup log must also be kept of all backup and recoverability testing done. The responsible official for updating of the backup log is the IT Support Officer.

7. BACKUP MEDIA STORAGE LOCATION

All backup data shall be stored in an onsite as well as an offsite storage location. Offsite storage of the backup data will be stored at the offsite backup server at the Disaster Control Room

Address: **Culvert Road, Pixley ka Seme District Municipality
DE AAR**

8. POLICY REVIEW

The Corporate Services Department (through the IT Support Officer) is the implementing authority of this policy and its subsequent review which will take place as new systems are introduced which requires its data to be backed up. Council must approve the policy, thereafter it will become the official policy of the municipality. **Council's** appointed officials and Contractors must follow the prescripts of this and other related policies to ensure its successful implementation.



EXECUTIVE MAYOR:



DATE APPROVED:

2026-05-28

RESOLUTION:

2026-05-28 (15.1)