SOL PLAATJE LOCAL MUNICIPALITY

EFT POLICY

APPROVED ON THE

RESOLUTION NUMBER

C15/04/26

Table of Contents

1. Policy Purpose

The primary goal of this policy is to ensure Electronic Funds Transfers (EFTs) are initiated, executed, and approved in a secure manner. This policy establishes requirements with respect to domestic payments via EFT for payments of municipal suppliers, monthly wage bill and adhoc payments as they fall due.

This policy applies to refunds made to municipal debtors arising from overpayments or credits passed in line with Customer Care, Credit Control and Debt Collection Policy of the municipality.

2. Definitions

Automated Clearing Bureau (ACB: Generally, refers to payments made via direct deposit and should be set up in the vendor master that denotes this payment method.

Banking information: Information from the payee or their bank regarding their account; including bank name, account name, account number, bank contact information and any other information necessary to transfer funds.

Electronic Funds Transfer (EFT): The electronic exchange (transfer of money from one bank account to another), either within a single financial institution or across multiple institutions, through computer-based systems. Wire transfers and ACB payments are examples of EFTs.

3. Applicable Legislation

MFMA Section 10 & 11 — controls over municipal bank accounts and withdrawals.

MFMA Section 62(1)(c) — requires internal controls that enforce “effective, efficient and transparent financial management”.

MFMA Section 65 – Expenditure Management

Section 55 of the Municipal Systems Act 32 of 2000

4. General Requirements

All EFT payments will be coordinated and submitted through Supply Chain Management, Payroll or Creditors Controller's Office. The Controller or his/her designee will approve all new and changes to electronic funds transfer requests, ensuring that the payment via wire is necessary, all required documentation is provided and appropriately approved, and that the request and banking account information is accurate and valid.

Change in banking details by a supplier must be done through the Central Supplier Database and Supply Chain Management (SCM) must be provided with the stamped bank account confirmation letter, for record keeping. The designated SCM official of the municipality is authorised to update any supplier bank account records, on the financial management system of the municipality.

For staff related banking details, changes can only be effected upon presentation of the stamped bank account confirmation to the Human Resource Department. Project workers banking details

are uploaded and/or updated by Payroll Office. No changes will be effected unless the employee presents himself/herself with proper identification. Telephonic, faxed or e-mail letters shall not be accepted.

5. Roles and Responsibilities

Accounts Payable in the Controller's office is responsible for ensuring that proper documentation, authorization and accounting information are provided and accompany any EFT payment instructions.

Supply Chain Management Acquisitioning is responsible for administrative process for the purchase of goods and/or services and negotiating payment terms in relation to those purchases.

The Controller's Office (Payroll or Creditors) is responsible for initiating and releasing EFTs on behalf of the municipality. Two separate individuals are required to initiate and release EFT payments through the municipality's banking partner's computer-based system. The Controller's Office also has the responsibility to confirm EFT instructions with specific departments and individuals if there is any question as to the validity of the EFT request.

Departments are responsible for obtaining and submitting proper support and approvals, including the completed and approved vouchers or payment documents at least thirty (30) calendar days prior to payment being needed.

Manual upload of payment on the banking application should be prohibited, and only automated upload of banking files will be accepted for releasing. This effectively means that all payments must first be processed and authorised on the financial or payroll system before payments may be released under normal procedures.

6. EFT Procedures

To promote the safety of the municipality's funds in the EFT environment, the following procedures will be adhered to:

- The procedure to initiate an EFT is subject to the same financial policies, procedures and controls that govern disbursement by any other payment mechanism.

- EFT transactions will not be made without proper authorization of affected parties in accordance with the municipality's procurement and recruitment business and billing refund practices.

- Authentication of new EFT requests and changes to existing EFTs required prior to the transaction being input into the computer-based banking system and includes the following steps:

    a) **Validate and verify** all electronic payment instruction requests received and confirm the correct account name and account number information.

b) **Document** the verification process that was followed to validate payment instructions. A record of the verification must be maintained in accordance with record retention policies.

- When EFT payments are approved, they will be set-up in the vendor master database in the financial accounting system by individuals authorized to perform vendor maintenance.

- Bank balances will be monitored daily for unusual or unexpected transactions. Bank statements in pdf format must be saved electronically and hard copies must be filed for audit purposes.

- Reconciliation of banking activity to the general ledger will be accomplished in a timely manner with investigation and resolution of reconciling items. A monthly bank reconciliation statement must be signed, must be saved electronically and must be filed for audit purposes.

- All municipal officials assigned with the powers and functions to release payments shall ensure that there is independence in decision making regarding authorisation of each payment. Releasers must verify that the releasing file generated from the financial system correlates with the imported bank file, prior to the releasing of any funds.

- Staff are fully aware of the extent of this responsibility and must exercise caution at all times to avoid financial losses by the municipality as well as litigation that may arise as a result of failure to pay all dues within the agreed upon timeframes.

- In a case of uncertainty with any payment, all enquiries must be referred to the Chief Financial Officer, who may in turn liaise with the department that was financially enriched by the services of the service provider.

7. User Access Management Processes and procedures

a) Management will immediately submit an item to the next Council meeting for any new appointments; service terminations or amendments to viewing rights
b) Creation, modification and deactivation of operators will be performed by the designated self-administrator. An EFT User Access form must be authorised and an activity log report must be printed to ensure a proper audit trail for auditing purposes.
c) Secure password reset protocols
    i. Require the supervisor's approval on the EFT User Access form.
    ii. The operator initiates the reset request via e-mail.
    iii. Telephonically verify Identity via employee number and ID number.
    iv. An activity log report must be printed, and the authorised EFT User Access form must be filed to ensure a proper audit trail for auditing purposes.
d) Conduct quarterly reviews of user access using system-generated reports, if available.
e) Conduct quarterly reviews on the monitoring of system administrator activities to ensure accountability.

8. IT Security

a) All operators that will be using the EFT system must be trained on the system. Operators must confirm and sign that they have received the necessary training.
b) Their computers need to be updated with the latest Java updates.

c) A security certificate which is unique to that particular user must be installed on that particular computer and/or laptop.
d) Operators using mobile devices must ensure that they adhere to the prescribed security protocols.
e) Users must have secure password and should not share it with anyone and the password must be changed according to the change management procedure of the designated bank.
f) All security mechanism or procedures implemented by the designated bank must be adhered to by users at all times.
g) Failure to comply to any assigned security prescripts by the designated bank may result in disciplinary action being instituted or dismissal.
h) Adhere to the multi-factor authentication and password requirements as per the banking system requirements - an account will be locked out, if the operator entered the wrong password 3 times and an account will be disabled for more than 90 days of inactivity.
i) All banking EFT files will be automatically saved via the financial system to a secure server/drive
j) Only first releasers in the Payment Section will have authorized access to this secure server/drive
k) Users that have authorised access to the secure server/drive will be reviewed on a quarterly basis and ensure that system logs are retained.

9. Policy Review

This policy shall be reviewed annually.

10. Implementation

This policy comes into effect from the date of approval.