

PROVINCIAL TREASURY • PROVINSIALE TESOURIE
• UNONDYEBO WEPHONDO



T13/2/2/3

D Coetzee

TREASURY CIRCULAR NO. 29/2010

THE PREMIER

THE MINISTER OF AGRICULTURE AND RURAL DEVELOPMENT
THE MINISTER OF COMMUNITY SAFETY
THE MINISTER OF CULTURAL AFFAIRS AND SPORT
THE MINISTER OF EDUCATION
THE MINISTER OF FINANCE, ECONOMIC DEVELOPMENT AND TOURISM
THE MINISTER OF HEALTH
THE MINISTER OF HOUSING
THE MINISTER OF LOCAL GOVERNMENT, ENVIRONMENTAL AFFAIRS AND DEVELOPMENT PLANNING
THE MINISTER OF SOCIAL DEVELOPMENT
THE MINISTER OF TRANSPORT AND PUBLIC WORKS
THE SPEAKER: PROVINCIAL PARLIAMENT
THE DEPUTY SPEAKER: PROVINCIAL PARLIAMENT

For information

ALL OTHER MEMBERS OF PARLIAMENT

THE ACCOUNTING OFFICER: VOTE 1: PREMIER (ADV B GERBER)
THE ACCOUNTING OFFICER: VOTE 2: PROVINCIAL PARLIAMENT (MR P WILLIAMS) (FOR INFORMATION)
THE ACCOUNTING OFFICER: VOTE 3: PROVINCIAL TREASURY (DR JC STEGMANN)
THE ACCOUNTING OFFICER: VOTE 4: COMMUNITY SAFETY (DR GA LAWRENCE)
THE ACCOUNTING OFFICER: VOTE 5: EDUCATION (MS P VINJEVOLD)
THE ACCOUNTING OFFICER: VOTE 6: HEALTH (PROF KG HOUSEHAM)
THE ACCOUNTING OFFICER: VOTE 7: SOCIAL DEVELOPMENT (MS K LUBELWANA)
THE ACCOUNTING OFFICER: VOTE 8: HOUSING (MR M TSHANGANA)
THE ACCOUNTING OFFICER: VOTE 9: ENVIRONMENTAL AFFAIRS AND DEVELOPMENT PLANNING (MR R ELLIS)
THE ACCOUNTING OFFICER: VOTE 10: TRANSPORT AND PUBLIC WORKS (MR J FOURIE)
THE ACCOUNTING OFFICER: VOTE 11: AGRICULTURE (MS J ISAACS)
THE ACCOUNTING OFFICER: VOTE 12: ECONOMIC DEVELOPMENT AND TOURISM (MR S FOURIE)
THE ACCOUNTING OFFICER: VOTE 13: CULTURAL AFFAIRS AND SPORT (MR B WALTERS)
THE ACCOUNTING OFFICER: VOTE 14: LOCAL GOVERNMENT (DR H FAST)

THE CHIEF FINANCIAL OFFICER: VOTE 1: PREMIER (MR P O'BRIEN)
THE CHIEF FINANCIAL OFFICER: VOTE 2: PROVINCIAL PARLIAMENT (MR R HINDLEY) (ACTING) (FOR INFORMATION)
THE CHIEF FINANCIAL OFFICER: VOTE 3: PROVINCIAL TREASURY (MR A GILDENHUYS)
THE CHIEF FINANCIAL OFFICER: VOTE 4: COMMUNITY SAFETY (MR M FRIZLAR)
THE CHIEF FINANCIAL OFFICER: VOTE 5: EDUCATION (MR L ELY)
THE CHIEF FINANCIAL OFFICER: VOTE 6: HEALTH (MR A VAN HUIKERK)
THE CHIEF FINANCIAL OFFICER: VOTE 7: SOCIAL DEVELOPMENT (MR JO SMITH)
THE CHIEF FINANCIAL OFFICER: VOTE 8: HOUSING (MR D BASSON)
THE CHIEF FINANCIAL OFFICER: VOTE 9: ENVIRONMENTAL AFFAIRS AND DEVELOPMENT PLANNING (MR AA GAFFOOR)
THE CHIEF FINANCIAL OFFICER: VOTE 10: TRANSPORT AND PUBLIC WORKS (MR CR ISMAY)
THE CHIEF FINANCIAL OFFICER: VOTE 11: AGRICULTURE (MR F HUYSAMER)
THE CHIEF FINANCIAL OFFICER: VOTE 12: ECONOMIC DEVELOPMENT AND TOURISM (MS M ABRAHAMS)
THE CHIEF FINANCIAL OFFICER: VOTE 13: CULTURAL AFFAIRS AND SPORT (MS BG RUTGERS)
THE CHIEF FINANCIAL OFFICER: VOTE 14: LOCAL GOVERNMENT (MR D BASSON)

THE HEAD OFFICIAL: PROVINCIAL TREASURY (DR JC STEGMANN)
THE HEAD: BRANCH FISCAL AND ECONOMIC SERVICES (MR H MALILA)
THE HEAD: BRANCH GOVERNANCE AND ASSET MANAGEMENT (MR TC ARENDSE) (ACTING)
THE HEAD: PUBLIC POLICY SERVICES (MR A PHILLIPS)
THE HEAD: PUBLIC FINANCE (MR H MALILA) (PRO TEM)
THE HEAD: FINANCIAL GOVERNANCE (MR A REDDY) (ACTING)
THE HEAD: ASSET MANAGEMENT (MR TD PILLAY)
THE CHIEF AUDIT EXECUTIVE (MS H ROBSON)
THE CHIEF FINANCIAL OFFICER (MR A GILDENHUYS)
THE SENIOR MANAGER: HUMAN RESOURCE MANAGEMENT (MS CM MILES) (ACTING)
THE SENIOR MANAGER: ACCOUNTING SERVICES: PROVINCIAL GOVERNMENT (MR N VAN NIEKERK) (ACTING)
THE SENIOR MANAGER: ACCOUNTING SERVICES: LOCAL GOVERNMENT (MS M FORTUIN) (ACTING)
THE SENIOR MANAGER: CORPORATE GOVERNANCE (MR B VINK)
THE SENIOR MANAGER: INTERNAL AUDIT: GOVERNANCE AND ADMINISTRATION CLUSTER (MS B CAIRCROSS)
THE SENIOR MANAGER: INTERNAL AUDIT: SOCIAL CLUSTER (MR M MALULEKA)
THE SENIOR MANAGER: INTERNAL AUDIT: ECONOMIC CLUSTER (MR J RADEBE)
THE SENIOR MANAGER: BUDGET MANAGEMENT: PROVINCIAL GOVERNMENT (MS M SHERATON)
THE SENIOR MANAGER: BUDGET MANAGEMENT: LOCAL GOVERNMENT (MR ML BOOYSEN)
THE SENIOR MANAGER: PROVINCIAL GOVERNMENT FINANCE (MS A PICK)
THE SENIOR MANAGER: LOCAL GOVERNMENT FINANCE (GROUP ONE) (MR E JOHANNES) (ACTING)
THE SENIOR MANAGER: LOCAL GOVERNMENT FINANCE (GROUP TWO) (MR M SIGABI)
THE SENIOR MANAGER: PUBLIC FINANCE POLICY RESEARCH AND MODELLING (MS C HORTON)
THE SENIOR MANAGER: IMMOVEABLE ASSET MANAGEMENT (MR NB LANGENHOVEN)
THE SENIOR MANAGER: MOVEABLE ASSET MANAGEMENT (MS N EBRAHIM)
THE SENIOR MANAGER: SUPPORTING AND INTERLINKED FINANCIAL SYSTEMS (MR A BASTIAANSE)
THE HEAD: OFFICE OF THE MINISTRY (MS A SMIT)

THE PROVINCIAL AUDITOR

MASTER RECORDS OFFICIAL: FINANCIAL MANAGEMENT

PRIVAATSAK X9165 PRIVATE BAG X9165
KAAPSTAD 8000 CAPE TOWN 8000
Telefoon (021) 483-Number Telephone (021) 483-Number
Faks (021) 483-Number Fax (021) 483-Number

THE UTILISATION AND MANAGEMENT OF THE OFFICIAL BANKERS SYSTEM

1. PURPOSE

The purpose of this policy is to outline the roles and responsibilities of the Departmental Service Administrator, Provincial Treasury and the Official Banker in the effective management of user accounts and the beneficiary master file, as well as the optimal utilization of the official bankers system.

2. INTRODUCTION

- 2.1 The official bankers system currently in use is Netbank Business. The day-to-day operation of the system (user access, payments, direct transfers, bank reconciliation, etc) is the responsibility of each Department, executed by Departmental users, appointed by the Accounting Officer/Chief Financial Officers, as authorized users of the system.
- 2.2 The Provincial Treasury, in addition to being in control of the Provincial Revenue Fund (PRF), which includes the Paymaster-General accounts of departments, render a support service to all Provincial Departments and further provide the linkage between departments and the official banker.
- 2.3 Vital to the integrity of the official bankers system is the institution and management of proper systems control. Weak systems controls, if prevalent, severely diminish the reliability of other internal controls associated with an application. Without effective system controls, other controls may be rendered ineffective by override, circumvention or modification. Such internal controls are indeed the controls that are established to ensure the accuracy, completeness and validity of transactions.
- 2.4 Previous assessments, reviews and audits have highlighted a lack of effective management of the official bankers system that could possibly lead to monopolizing of imported data, unauthorised usage of tokens and irregularities/fraud. The main areas of concern highlighted includes the following:
 - Departmental policy is not in place to guide and direct access to the system (who gets access and under which condition)
 - No clear documented departmental procedures and defined responsibilities for the management of system users (approval, termination, dormant, etc)
 - Functions executed on the systems by departmental users are seldom in line with their job descriptions
 - The Beneficiary master file not maintained on a regular basis
 - Files imported into the banking system not secured
- 2.5 Therefore to ensure that the official bankers system is professionally managed, access control properly executed, access and logon violations timeously identified and reported on and that policies are in place to guide and direct access, the guidelines, procedures and processes as outlined in this policy document must be adhered to.

3. PROCEDURES/POLICIES TO BE IMPLEMENTED WITH IMMEDIATE EFFECT

3.1 Applicability

This Policy is applicable to all Provincial Departments within the Provincial Government of the Western Cape (excluding Provincial Parliament) and does not replace the departmental policy that must be in place to guide and direct access and define responsibilities for the management of systems on departmental level.

4. ACCESS CONTROL

4.1 New users

- The Accounting Officer/Chief Financial Officer is responsible for the appointment of a Service Administrator and users of the Banking System.
- When appointing a user the Chief Financial Officer must ensure that prescripts and procedures relating to access control are in place and adhered to. To limit risk only a limited amount of officials must be given access to the Banking System
- New users will only be granted access to the system upon receipt of a request signed by the Chief Financial Officer indicating the following:
 - Departmental Profile
 - Name of official
 - ID number (certified copy of id)
 - Pearsal number
 - Telephone-; Fax number and e-mail address
 - Access to which accounts
 - Type of access (1st or 2nd authorizer, capturer, Administrator)
 - Functions to be allocated

It is important to note that the application must reflect all relevant information to ensure that a new user is created correctly. The Chief Financial Officer must further ensure that the request for a new user is in line with their job description and that segregation of duties does exist.

4.2 Changes to access rights

- A request signed by the Chief Financial Officer indicating the following must be forwarded to the Provincial Treasury:
 - Departmental Profile
 - User name
 - User id
 - Indication of new access rights

4.3 Passwords

- General:
Passwords are solely for the relevant user's access to the system and must be used in a responsible manner and never shared with any other person under any circumstances. A "complex password", consisting of alpha, numeric and special characters (eg. *,%,& etc) must be utilized at all times. A password will be case-sensitive and may not contain any characters that are repeated three times or more.

- Standardise password length:
Systems in general, provide for a minimum and maximum password length. The maximum password length provided for by the banking system is 16 characters.
- Standardise password expiry period:
The password expiry date is preset to 90 days. To further limit the risk of identification it is recommended that the system users change their passwords on a monthly basis.
- Reset:
The user will contact the Nedbank Helpdesk (0861 555 221) to reset the password if he/she can remember the password (was typed incorrectly). Three consecutive errors will result in a user's access being suspended until reset.
- Re-issue:
A request indicating the departmental profile; user name/id , reason(s) for re-issue and signed by the Chief Financial Officer must be sent to the Provincial Treasury requesting the re-issue of a password. When the Provincial Treasury receives the new password the user will have to sign for the sealed envelope containing the password.

4.4 Tokens

- Netbank Business, in addition to the normal security aspects, utilizes a device known as a token to further limit the possibility of unlawful access to the banking system.
- Tokens must under no circumstances be handed over or transferred to another official.
- Tokens are solely the responsibility of the relevant user(s). Tokens should at all times be kept in a safe place. If a token is no longer used by an user, the user must return the token to Provincial Treasury, Financial Asset Management, Third floor, 7 Wale Street, Cape Town
- Departments to ensure that any unused tokens are returned to the Provincial Treasury.

4.5 Deactivate dormant users in service as well as users who have left the service:

Users registered on the banking system who have not accessed the system for long periods, have been promoted or rotated within the department, who do not render that specific system function anymore and users that have left the service of the department, must be deactivated. It is the responsibility of the Departmental System Administrator to inform the Provincial Treasury by means of a letter signed by the Chief Financial Officer indicating the Departmental Profile, user name and user id to be deactivated. The following users must be deactivated:

- System users who are on leave for periods exceeding 30 days (maternity; study; overseas, special leave; etc.) must be deactivated at the start of their leave period and activated again upon their return.
- Users who have been promoted or rotated within their departments and do not perform that specific function anymore;
- Users who have left the service of the department.

Departments must review all user accounts on a quarterly basis. Service Administrators must provide written confirmation to Provincial Treasury that all active users on the system

are a true reflection of the departmental officials permitted access to the system in accordance with their job descriptions.

4.6 Relief Service Administrator

- A relief Service Administrator must be appointed in the event of the Service Administrator being absent from work and Provincial Treasury must be informed in writing before the Relief Service Administrator, resumes duty.

5. **BENEFICIARY LISTS**

Payments are made against the bank account detail contained in beneficiary lists, therefore it is important to ensure adequate approval and change control over these profiles. The function of maintaining beneficiary lists should be performed by officials not involved with capturing and authorizing of payments on the banking system. This is to ensure proper segregation of duties and to reduce the risk of payments against unauthorised or incorrect bank account numbers. When changes must be made on banking details, original documentation must be provided by the beneficiary and an audit trail must be printed of changes made and filed with the request for the change.

Account Verification Services (AVS)

- Nedbank has implemented an AVS, that will be activated at departments during June 2010
- AVS allows Business Banking users to verify that the details of an account and the account holder correlate to the risk of fraudulent redirection of funds.
- The key benefits of AVS are risk reduction and cost savings
- The following data fields will be verified:
 - * The account number (current or savings) is valid
 - * The ID number or company registration number specified belongs to the account number
 - * The initials and surname match
- The following information must be available for Account Verification to be done:
 - * Account Type (Current/Savings)
 - * Account number
 - * Branch code
 - * ID Number/Company registration number
 - * Surname/Company name [Account name]
 - * Initial(s)
- The following banks currently form part of the AVS
 - * Nedbank
 - * ABSA
 - * Standard Bank
 - * FNB
 - * Capitec
 - * Merchantile Bank
 - * African Bank

6. IMPORTING OF FILES IN ORDER TO MAKE PAYMENTS

Electronic importing of payment transactions are protected from unauthorised tampering by security controls, such as encryption. An unsecure file increases the risk of information being amended and unauthorised payments being created. The imported file must be approved on the Banking system and reconciled from the source to the Banking system, therefore:-

- When a department wishes to make use of the import function on the Banking System they must ensure that the following are in place:
- Use a secure interface method [eg. Automatic Clearing Bureau (ACB), Comma separated value (CSV)]
- Ensure segregation of duties between the importing of the file from the source system and the authorisation on the Banking System.

7. STATEMENTS AND AUDIT TRIALS

- After transactions have been captured and authorized on the Banking system a bank statement and audit trail (proof of payment/transfer) must be printed. This will assist with the cash flow reconciliation purposes to ensure all payments were processed and the correct banking details were used.
- Original copies (incl E-statements) of Bank statements must be kept for Audit purposes for a period of five (5) years.

8. CONCLUSION

- Your assistance to ensure the effective and efficient management of the banking system and compliance to the prescripts will be greatly appreciated.
- This policy will be revisited on at least an annual basis and revised if required.



MANAGER: FINANCIAL ASSET MANAGEMENT
DP ALEXANDER



ACTG SENIOR MANAGER: SUPPORTING AND INTERLINKED FINANCIAL SYSTEM
R ESACK

DATE: 2010.08.03