

**LIMPOPO PROVINCE  
DEPARTMENT OF LOCAL  
GOVERNMENT AND HOUSING**



**FINANCIAL  
SYSTEMS  
POLICY**

# INDEX

**PART A: PERSAL**

**PART B: BAS**

**PART A: SYSTEMS MANAGEMENT**

1. OBJECTIVE

2. PREAMBLE

3. MANDATES

4. ACCESS CONTROL

5. SECURITY MANAGEMENT

6. USER SUPPORT

7. DEACTIVATION OF USERS

8. FUNCTIONAL MAINTENANCE

## 1.OBJECTIVE

The purpose of this policy is to provide a uniform guideline regarding the access ,processing of transactions as well as security measures in the management of financial systems within the Department of Local Government & Housing in order to meet the strategic goals of the department and comply with the Public Finance Management requirements and Treasury Regulations and further adhere to the stipulations of Electronic Communication and Transaction Act.

## 2.PREAMBLE

- The government of South Africa is accounting for its financial transaction through the BAS system and account for its compensation and record of employees through the Persal system.
- To ensure the uniform implementation of the norms and standards

## 3.MANDATES

Electronic Communication and Transaction Act, Act 25 Of 2002

- Public Service Regulation
- Public Finance Management Act No:1 Of 1999
- Treasury Guidelines


## 4.ACCESS CONTROL

### 4.1.PART A: PERSAL ACCESS SECURITY

- The Persal access control requirements and standards aims to ensure that computer resources and the integrity of data is protected at all times.
- Since user profiles are regarded as electronic signatures as outlined in the Electronic Communication and Transaction Act, Act 25 of 2002

. This notice is intended to ensure that:

- Only authorized individuals are granted appropriate system access to perform their duties while minimizing the risk of the data or systems being compromised.
  - Authorized individuals properly access and utilize the data and systems.
  - Authorized individuals properly maintain confidentiality of all data and systems.

 PERSAL Controllers are accountable for instating, maintaining and communicating procedures to ensure the continuous control over of access security in departments

Such procedures should be specific in that PERSAL USERS are held fully responsible for protecting their own ID'S and passwords.



- Access to PERSAL requires two layers of security namely:
  - .Mainframe access (first ID, mainframe ID, RACF ID, Complete ID, LHL001) and; PERSAL access (second ID, user ID, PERSAL ID, Q20001).

### **Mainframe Access (Complete Id's)**

- In order to obtain access to the PERSAL system a user must have a COMPLETE ID
- and a PERSAL user ID. The COMPLETE ID is supplied by the relevant bureau (BEREAU NUCLEUS)on
- which the department or province is operating on. This COMPLETE ID is used to
- access to PERSAL system via the RACF environment, after which the PERSAL
- access security control, is applied on the PERSAL system for the specific PERSAL
- user ID.
- Departments and Provinces are responsible to put security controls in place for
- these ID`S and to implement best practices for IT governance as per departmental password security policy

### **PERSAL SYSTEM FUNCTIONALITY**

- The system is standardized for all the National government departments and Provincial Administrations, including the

SAPS and Correctional Services. This ensures better control and the facility to provide quick and accurate response to high level enquiries.

- The operation of the system is menu driven and the menus are set up dynamically according to the access security profile of the user. Online help is available for all the screens and there is a full user manual that is maintained on the system.
- The system is operated online and full online validation is done to ensure data integrity. Transactions are written to a suspense file with approval and authorization functionality. The transactions are then processed and the relevant data is updated. Recalculation of salary data is done during this process in order to have up-to-date data available.
- The system is fully integrated between the personnel -and salary sub systems to ensure that capturing of data is only done once. If personnel data is captured that has a financial implication, e.g. promotions, the salary data will be updated accordingly. A full audit trail / stamp is kept of all actions performed on the system.
- The system has interfaces with other systems which include financial institutions, educational institutions, employee institutions, medical funds, pension funds, insurance companies, Automated Clearing Bureau and financial systems.



## MAINTENANCE OF THE PERSAL SYSTEM

- Maintenance requests on the system are controlled and monitored through the SCC (System Change Control) system. The SCC system is online and the users or functional support personnel register requests for changes or enhancements to the system. All system changes, even changes that originate from changes in policy, are registered on the SCC system.
- The flow of an SCC and drafting of specifications for the specific SCC is in strict accordance with the procedures as set out in detail in PERSAL-STD-0002 – PERSAL Standards and Guidelines.
- System changes are made at Bureau Beta, which is the development bureau, and are distributed to the other production bureaux. Maintenance is done according to the BSM (Business Standards Management) system of Business Connexion, an ISO9001 certified company.
- Maintenance of the bas system are controlled and monitored the system change controllers who is constituted of members from different department, they present their recommendation in the national bas user forum for ratification. Upon ratification the recommendation will be sent to the technical team for design and implementation





## 5. SECURITY MANAGEMENT IN BAS SYSTEM

- Due to the sensitive nature of the accounting system and the number of users using the system, it is necessary to include various security features to prevent misuse of the system.
- This is accomplished by means of:
- Individual User ID's for every person utilizing the system;
- Self-chosen passwords for each individual that expire after a predetermined period i.e.30 days.
- The ability to deactivate or activate individual User IDs;
- Immediate BAS Function locking facility; and
- Limited number of login attempts only 3 attempts
- Each user of the system is given a certain level of authority/clearance based on the tasks they need to perform their jobs and, depending on which level of clearance they have, are assigned access to a Group. This Group is set up and maintained by the Systems controller.

A Group is made up of certain BAS Functional Areas. If a user is a member of a Group he/she will have access to all the Functional Areas belonging to the Group. Functional Areas equate roughly to items in the pull down menus of the BAS main window, hence users assigned to a specific Group will only have



access to the menu items associated with that Group. It is possible to merge two or more groups, thereby forming a new "merged" group which has the characteristics of all the groups it was merged from.

- While users are linked to Groups that control the access to BAS functional areas, their access to the Code Structure is individually controlled. e.g. Two Receipts clerks may be members of a Group that allows them access to the "Receipts" function, yet one may only be allowed to access "assets and liabilities" while the other only has access to "Debt Repayments" items

## 6. USER SUPPORT

- The system controller or his/her assistant shall be the first line of contact to render the support.
- The system controller/assistant shall attend the provincial and national user forum to be abreast with the development pertaining to the systems.
- System developments/enhancement will be communicated through the notices and messages for information and implementation.
- The controllers will disseminate and monitor the implementation of such notification.

- All the de-activate access to the systems shall be re-setted by the controller upon completion of the relevant reset forms obtainable in the following web sites.
- <http://persal.pwv.gov.za> and <http://bas.pwv.gov.za>. telephone LOGIK call center
- 012 657 4444 and Provincial support at ip address 10.8.131.247 and 015 291 8598/ 015 291 8683/ Departmental is 015 294 2116 and [semenyaal@limdlgh.gov.za](mailto:semenyaal@limdlgh.gov.za)

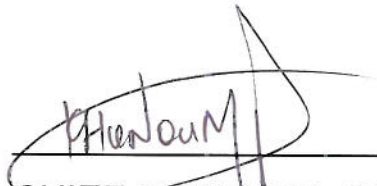
## **7.DEACTIVATION OF THE USERS**

The system controller shall deactivate the user upon notification from the supervisor that the user is no longer in service.

The supervisor will de-activate the user if there are investigation taking place.

## **8. FUNCTIONAL MAINTENANCE**

Both system controllers and GITO has co-responsibilities to make sure that the systems functions to their maximum capacity within the stipulated parameters

  
CHIEF FINANCIAL OFFICER

Approved / Not Approved



HEAD OF DEPARTMENT

Date: 30/08/2009

