

PROVINCE OF THE EASTERN CAPE



Department of Rural Development and Agrarian Reform

PERSAL USER MANAGEMENT POLICY

2024

TABLE OF CONTENTS

| | |
|--|-----------|
| DEFINITIONS AND INTERPRETATION OF TERMS..... | 1 |
| 1. INTRODUCTION..... | 3 |
| 2. OBJECTIVES | 3 |
| 3. REGULATORY FRAMEWORK..... | 3 |
| 4. SCOPE OF APPLICABILITY..... | 4 |
| 5. ROLES AND RESPONSIBILITIES | 5 |
| 6. PERSAL ACCESS SECURITY CONTROL/USER REGISTRATION | 8 |
| 7. DISCLOSURE OF PERSAL INFORMATION/CONFIDENTIALITY | 9 |
| 8. PERSAL TRAINING | 9 |
| 9. USER ACCOUNT MANAGEMENT | 10 |
| 10. AUDITING OF DEPARTMENTAL PERSAL USERS..... | 10 |
| 11. MONITORING, EVALUATION AND CONTROL | 11 |
| 12. POLICY REVIEW..... | 11 |
| 13. RECOMMENDATIONS & APPROVALS | 11 |

DEFINITIONS AND INTERPRETATION OF TERMS

For the purpose of this policy document meanings and the definitions of terms are provided below: -

“Authoriser” means a user responsible for approving transactions using function #6.8.30 after the relevant transaction has been approved by the reviser.

“Alphanumerical” means a word made up using a combination of letters of the alphabet and numbers.

“Complete user id” means the ID allocated to a user in order to log on to the mainframe which houses Persal.

“DRDAR” means the Department of Rural Development and Agrarian Reform

“Exception reports” means reports which are generated programmatically by the system, and reflect those instances where records or transactions do not comply with the required data criteria of the system.

“IP Address” means a 32-bit address used to identify a node on an IP internetwork. Each node on the IP internetwork must be assigned a unique IP address, which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). The IP address can be configured either statically or dynamically through DHCP.

“PC” means a Personal Computer

“Password” means a secret word a Persal User must use in order to access the Persal System.

“Persal” means the Personnel and Salary System in the Public Service.

“Personnel/salary controller” means an official who is responsible for registering and maintaining user profiles of users under his/her control, and also for ensuring that users are equipped with the tools to perform their duties effectively and efficiently on the Persal System.

“Persal manual” means a manual providing help for the day-to-day usage of functions on the Persal System.

“Persal number” means a unique system generated 8-digit number assigned to

each employee who is appointed on the Persal System.

"Persal User Id" means the Id allocated to a User, to log on to the Persal System.

"Reports" mean management information extracted from the Persal System by means of ad-hoc or pre-programmed system reports.

"Reviser" means a Persal user who is responsible for checking and approving another user's work.

"Revoked" means that access to the Persal System has been temporarily suspended.

"SITA" means State Information Technology Agency.

"Static IP address" means a fixed IP address.

"System Change Control (SCC)" means a request made by certain authorised users for changes/modifications to be made to the Persal System.

"Transmission Control Protocol/Internet Protocol" means a set of networking protocols widely used on the internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for networks and routing traffic.

"User" means any employee who has authority and a user ID to access the PERSAL System

1. INTRODUCTION

1.1 Background

PERSAL is purely the existing Human Resources and Salary System for Government with a fully integrated Human resources and Payroll functionality. This means that PERSAL is the system that is currently being utilized in the Public Service to process all salaries of employees and act as a database to store all Human Resource and salary related information.

1.2 Problem statement

Currently there are no formal provisions to guide and direct access to the PERSAL System in the Department. There are no formal guidelines and directives to assist in the management and prevention of fraud and corruption on the PERSAL system in order to minimize risk. Also there are no clear roles and responsibilities for all role-players who are managing and utilizing the PERSAL System. Furthermore, analysis of queries referred to the PERSAL Control Unit and LOGIK call centre as well as PERSAL audits indicate constraints among PERSAL users.

The purpose of this document is to provide Head Office, District Offices and Centres with a policy to regulate and manage the usage of the PERSAL system, within the Department of Rural Development and Agrarian Reform.

2. OBJECTIVES

The objectives of this departmental policy are as follows;

- 2.1 To stipulate and clearly define the roles and responsibilities of all role players towards utilization and management of the Persal System;
- 2.2 To ensure that the information/data captured and stored on the Persal System is accurate, credible, reliable, regularly audited and complies with the National Minimum Information Requirements (NMIR);
- 2.3 Stipulate the provisions relating to security access control;
- 2.4 To clearly define processes to assist in the management and prevention of fraud and corruption as a result of the manipulation of the Persal System by users;
- 2.5 Provide guidelines regarding Persal training and establish a well-trained Persal cadre/user group for the department.

3. REGULATORY FRAMEWORK

The mandate for the functional operation of Persal is mainly derived from:

- 3.1 Public Service Act, 1994, as amended (Act 103 of 1994),
- 3.2 Public Service Regulations, 2001,
- 3.3 Employment of Educators Act, 1998 (Act 76 of 1998),
- 3.4 Labour Relations Act, 1995 (Act 66 of 1995),
- 3.5 Employment Equity Act, 1998 (Act 55 of 1998),
- 3.6 Skills Development Act, 1998 (Act 97 of 1998),
- 3.7 Skills Development Levies Act , (Act 9 of 1999),
- 3.8 Medical Schemes Act , 1998 (Act 131 of 1998),
- 3.9 Short-term Insurance Act , 1998 (Act 53 of 1998),
- 3.10 Long-term Insurance Act , 1998, (Act of 1998),
- 3.11 Regional Services Council Act (Act 105 of 1985),
- 3.12 Usury Act 1968 (Act 73 of 1968),
- 3.13 Magistrates' Courts Act, 1944 (Act 32 of 1944),
- 3.14 Government Employees Pensions Law, 1996,
- 3.15 South African Qualification Authority Act, 1995,
- 3.16 Basic Conditions of Employment Act, 1997 (Act 75 of 1997),
- 3.17 Public Finance Management Act, 1999 (Act 1 of 1999),
- 3.18 Treasury Regulations, 2005,
- 3.19 Promotion of Access to Information Act, 2000 (Act 02 of 2000),
- 3.20 Protected Disclosure, 2000 (Act 26 of 2000),
- 3.21 Electronic Communications and Transactions Act, 2002 (Act 25 of 2002),
- 3.22 Unemployment Insurance Act 2001 (Act 63 of 2001),
- 3.23 Good Practice Guide on User Account Management issued by the Auditor General:
March 2010,
- 3.24 Directives Issued by:
 - a) The Department of Public Service and Administration
 - b) National Treasury
 - c) The South African Revenue Services
 - d) HR: Information Management (MIS)

4. SCOPE OF APPLICABILITY

- 4.1 The provisions of this policy document shall apply to all employees of the Department of Rural Development and Agrarian Reform and any third party official employed who utilizes the Persal System.

5. ROLES AND RESPONSIBILITIES

5.1 The efficient utilization and effective management of the Persal System must depend on the following role players: Persal Users, Persal Revisers, Persal Controllers (HR and Finance), Departmental Persal Controller and the Persal Manager.

5.2 Persal User.

5.2.1 There shall be Persal Users at district, head office and centres who will be responsible for the following:

- (a) Human Resource Planning (organization and establishment)
- (b) Personnel Administration
- (c) Salary Administration
- (d) Labour Relations
- (e) Human Resource Development
- (f) Self-Development

5.2.2A user shall only instate a transaction based on relevant source documentation and must ensure that the data captured on Persal is accurate. A Persal route form shall be used by all users to capture any type of data on the System.

5.3 Persal Reviser / Authorizer

A Persal reviser shall be responsible for:

5.3.1 Approval of suspense files transactions in terms of internal delegations and Public Service directives and/or internal departmental policies.

5.3.2 May only approve or authorize a transaction based on relevant valid source documentation that complies with reliability (accuracy, completeness and timeliness) and integrity (validity and authorization).

5.3.3 May not approve or authorize his or her own transaction.

5.3.4 May not compile data regarding his/her own transaction.

5.3.5 A Persal Reviser/Authoriser is subject to ongoing in-house training and self-development.

5.3.6 Must promote compliance with the National Minimum Information Requirements (NMIR), extracts and clear reports to monitor faulty, rejected transactions and transactions awaiting approval / authorization in respect of distributions under their control on a daily basis. All transactions with a financial implication that need authorization must be authorized by the relevant sections.

5.4 Persal Controllers (HR and Finance)

There shall be Persal Controllers for both HR and Finance in the districts, head office and centres who shall be responsible to:

- 5.4.1 Manage Persal in their respective Units / district/ centres.
- 5.4.2 Assess and record the Persal training needs of the Unit/District in conjunction with section heads, in order to make nominations for training courses, as and when required.
- 5.4.3 Facilitate the registration of new users and submit to the Persal Manager at head office.
- 5.4.4 Register and maintain user profiles for users and allocates specific functions in relation to their job descriptions and allocate revisers to users according to the work demands.
- 5.4.5 Link authorizers to relevant transaction codes and monitor the linkage between the users and revisers. After registering users, the controller must keep original Persal registration forms as distributed from the respective Users.
- 5.4.6 It is the function of the Controller to support Persal users at district/centre level and maintains the link between the district office and the Departmental Persal Controller.
- 5.4.7 Attend the half-yearly departmental Persal Users information sessions and ensure that issues discussed are followed-up or relayed to users under their control.
- 5.4.8 Extract reports to monitor faulty, rejected transactions and transactions awaiting approval/authorization in respect of distributions under his/her control.
- 5.4.9 On a monthly basis Persal Controllers shall audit all users under their control to verify if users are still in need of the functions allocated to them.
- 5.4.10 Notify the relevant unit about the exceptions that must be corrected on the System. In the event that the Controller is away for more than a month, his/her controller duties must be delegated to the Reviser.

5.5 Departmental Persal Controller

- 5.5.1 Manages and monitors Persal activities in the Department.
- 5.5.2 Registers and maintains user profiles for users and allocates specific functions in relation to their job description.
- 5.5.3 Allocates revisers to users as required.
- 5.5.4 Links authorizers to relevant transaction codes.

- 5.5.5 Monitors the linkage between the users and revisers.
- 5.5.6 Accounts for effective utilization of the Persal System in Department
- 5.5.7 Attends the quarterly Departmental Persal Users information sessions and ensures issues discussed are followed-up or relayed to all users.
- 5.5.8 Extracts reports to monitor faulty, rejected transactions as well as transactions which await approval/authorization in respect of distributions for the Department.
- 5.5.9 Monitors the suspense and transaction files and follows up questionable transactions.
- 5.5.10 Ensures that exceptions are verified, investigated and followed for corrective action.
- 5.5.11 Interacts with the BAS Controller to ensure proper interaction / interface between Persal and BAS and maintain and implement required changes.
- 5.5.12 Provides continuous support, guidance and training to all Persal role players within the Department.
- 5.5.13 Must subject him/her to ongoing in-house training for self-development purposes.

5.6 Persal Manager

- 5.6.1 Is responsible for giving strategic direction and planning for the unit.
- 5.6.2 Is responsible for the overall managerial, technical, system and user support and Persal training for the department.
- 5.6.3 Ensures that the work plan agreements for the unit are aligned to the performance indicators as identified in the Annual Performance Plan of the department.
- 5.6.4 Shall be responsible for the orientation of all users of the system.
- 5.6.5 Shall be responsible for the creation and maintenance of codes on the departmental code file.
- 5.6.6 Shall Manage and control Persal circulars and messages and bring important issues to the attention of all users in the Department.
- 5.6.7 Shall monitor and ensure the effective use of the Persal System.
- 5.6.8 Ensures professional, effective and efficient interaction between Head Office, and the Persal Controllers (HR and Finance) at district/centre level.
- 5.6.9 Implement Persal control and audit measures for the entire Department.
- 5.6.10 Ensure that Persal supports the personnel and salary management requirements of the department.

- 5.6.11 Evaluate and recommend/reject requested changes to the Persal System made through the System Change Control facility/tool.
- 5.6.12 Advises district/centres as to the functionality of the Persal System and reports that are available to support decision making on human resource information data.
- 5.6.13 Ensures compliance with the Persal User Management Policy, Persal Procedure manual and other relevant prescripts.
- 5.6.14 Chairs the Departmental Persal user information sessions and represents the Department at the National/Provincial Persal User Forum.

6. PERSAL ACCESS SECURITY CONTROL/USER REGISTRATION

There shall be formal user registration procedures for granting access to PERSAL as follows.

- 6.1 A formal documented access request form should be completed and approved by the user's supervisor.
- 6.2 The user access request form shall contain an undertaking by the respective users to be signed in black ink before access shall be given to the respective users.
- 6.3 The access request form shall make provisions for the new user to choose the relevant Persal functions and shall be approved by the supervisor.
- 6.4 The Persal Controllers shall have the right to refuse access, terminate or revoke a user's access to the Persal System.
- 6.5 The HR and the Salary Controllers shall ensure that the functions allocated to users are directly related to the user's job description with the exception of Persal report functions.
- 6.6 A formal request for additional functions shall be completed and submitted to the controller should the user require additional functions to be allocated.
- 6.7 The request to remove functions form shall be completed and submitted to the controller should the User changes his/her job description.
- 6.8 A Request for Linking of Transaction Codes form must be completed and submitted controller should the user requires to be linked to transaction codes.
- 6.9 A Request to Terminate a User form must be completed and submitted to the controller should the User be terminated from the system.

- 6.10 The respective HR and Salary Controllers must ensure that Users who exit the Department are terminated immediately on the day they leave. This is done for audit and security purposes.
- 6.11 For security reasons, it is recommended that each User must have his/her own Persal terminal to access the System.
- 6.12 Users shall log off each time they leave the terminal to prevent misuse of their Persal User ID's.
- 6.13 A User shall be strictly prohibited from utilizing the user ID of another employee.
- 6.14 A Persal Reset form shall be completed by the User and submitted to the Persal Controller, in order for the User ID's password to be reset and the original form must be filed for audit purposes.
- 6.15 All Persal forms in respect of all Persal Controllers as detailed above shall be sent to the Persal Management Unit for approval by the Persal Manager.

7. DISCLOSURE OF PERSAL INFORMATION/CONFIDENTIALITY

- 7.1 A User shall keep any information obtained by him/her through the use of the Persal system confidential and take all reasonable steps and precautions to ensure that such information remains strictly confidential.
- 7.2 No third party should obtain unauthorised access thereto. In this instance Persal users are referred to section 16 (5) (a)(c)(d) of the Labour Relations Act, 1995, (Act No. 66 of 1995). When attending to requests for verification of employment by a third party (e.g. Financial Institution, Insurance Institution or Debtor(s), the third party must provide all the information and the user may only affirm or refute the correctness of the given information.
- 7.3 The verification of employment shall be attended to at head office and District/centre level by the relevant sections e.g. HR/Finance. In order to obtain Persal information from the PERSAL Management Unit it is necessary for the request to be requested in writing, e-mail or fax.

8. PERSAL TRAINING

- 8.1 In order to promote a better understanding of Persal, ensure optimal utilization of the system and to minimize errors it is necessary to ensure that all Persal Users and Controllers are properly trained. This will also ensure that the Department has credible and reliable information on its employees that will contribute to informed decision-making in the Department.

- 8.2 A Departmental Training Requirement Database must be established which will be forwarded to Provincial Treasury to be included in their training program or schedule for each calendar year. Should there be an urgent training request that cannot be accommodated by the Provincial Treasury; alternative training measures shall be put in place either by means of internal in-house training or outsourcing the specific training requirement needs.
- 8.3 HR and Salary Controllers (Head Office and District/Centre level) shall submit their Persal Users Training requirements by completing the Persal Training Requirement Request form that shall be supplied by Provincial Treasury Persal training to the Departmental Persal Controller.

9. USER ACCOUNT MANAGEMENT

- 9.1 There shall be appropriate access control practices that must be put in place. Preventive measures should be implemented to minimize risks and manipulation of the Persal System. This will assist the Department of Rural Development and Agrarian Reform to achieve better Persal information security, responsibility and accountability.
- 9.2 User account management procedures must cover the life cycle of user access, starting from the initial registration of new users to the final deregistration of users who no longer require access to the Persal System. All user account management procedures shall be documented and formally approved as required.

10. AUDITING OF DEPARTMENTAL PERSAL USERS

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

The Persal Manager and Departmental Persal Controller shall ensure that:

- 10.1 Only authorized individuals are granted appropriate Persal System access to perform their duties while minimizing the risk of data or system being compromised and or manipulated.
- 10.2 Authorized individuals properly access and utilize the data on the system.
- 10.3 Authorized individuals properly maintain confidentiality of all data from the Persal system.

10.4 All Persal users shall be held fully responsible for protecting their own user ID's and passwords. This implies that Persal Users shall not be allowed and are strictly prohibited from exchanging, sharing or loaning each other their user ID's and passwords. All Persal users in the ECDRDAR are audited every month.

10.5 All Persal Users found not to be utilizing the Persal System more than a month shall have their user IDs terminated when identified.

11. MONITORING, EVALUATION AND CONTROL

11.1 All PERSAL Users shall be responsible for ensuring data integrity and preventing the misuse of the Persal System. The PERSAL Management Unit shall monitor activities on the System, report on their findings and ensure that corrective measures are implemented. The activities of the departmental Persal Controller/Manager shall be monitored by Provincial Treasury: Persal component.


12. POLICY REVIEW

12.1 This policy shall be assessed in five (5) years from its effective date to determine its effectiveness and appropriateness. This policy may be assessed before that time as necessary to reflect substantial organisational changes or any change required by law.

13. RECOMMENDATIONS & APPROVALS

~~APPROVED/NOT APPROVED~~

Comments: _____



MR. B DAYIMANI
ACTING HEAD OF DEPARTMENT
DATE: 28/03/2024