INFORMUS

FOR PSA MEMBERS: DEPARTMENT OF HOME AFFAIRS

17-08-2021

Update: Reviewed Persal system policy

The employer tabled a draft policy on Persal systems for consultation and inputs. The draft policy is aimed at regulating and giving directive regarding the human resources and salary information on the system.

The draft policy was subjected to the internal mandating process of the PSA, and it was found that there were no substantial changes made. However, the PSA wishes to request members to peruse the *attached* draft policy and submit inputs to peter.mngomezulu@psa.co.za by **26 August 2021**.

The PSA wants to take this opportunity to wish all employees who are unwell owing to COVID-19 a safe and speedy recovery.

GENERAL MANAGER

home affairs

Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA

PERSAL SYSTEM POLICY

(Personnel and Salary system)

BRANCH: HUMAN RESOURCE MANAGEMENT AND DEVELOPMENT

POLICY INFORMATION AND REVISION LOG

File Name	Persal System Policy
Original Author(s)	Branch: Human Resources Management and Development
Current Revision Author(s)	Directorate: People Benefits
Next Review Date	This Policy is subject to review as and when deemed necessary or required, to ensure that it is aligned to prevailing legislation, directives, guidelines, and / or operational requirements.

Version	**Date**	**Authors**	**Revision Notes**
0.1	28 November 2013	DHA: HRM&D	This version was integrated into the Persal Policy which was approved on 27 February 2014.
0.2	27 February 2014	DHA: HRM&D	Persal Policy approved on 27 February 2014.

POLICY RECOMMENDATION / APPROVAL

Recommending Authority		Ms ND Mohoboko
		Deputy Director-General: Human Resource Management & Development
Signature		
Date:		

Approving Authority		Mr LT Makhode
		Director-General: Home Affairs
Signature		
Date of approval		
Implementation Date		As per date of Approval / Implementation Directives

TABLE OF CONTENTS

1 PRELIMANARY

1.1 Purpose

1.1.1 As the Department of Home Affairs continues in its quest to position itself as a credible and high performing organisation, its responsibility to regulate and manage the utilisation of the Persal system to address the Department's Human Resource and Payroll requirements, is paramount.

1.1.2 This policy aims to ensure a uniform, fair and consistent approach to:

- Persal access management, and mitigation of identified risks;
- strengthening system security controls to ensure that Persal access and applications, are appropriately restricted, segregated, managed, monitored and controlled;
- the implementation of sound practices and procedures to improve data integrity (updated, timely, accurate and reliable) for the delivery of Persal Management Information; and
- establishing internal controls to enhance Corporate Governance and IT Governance practices.

1.2 Title / Commencement / Statutory Framework

This shall be called the Persal System Policy, and shall come into operation on a date duly authorized by the Director-General (DG).

2 LEGISLATIVE / POLICY FRAMEWORK

This Policy for the functional operation of Persal, is mainly derived from the following legislative / Policy Frameworks:

- Public Service Act, 1994 (Act 103 of 1994), as amended;
- Labour Relations Act, 1995 (Act 66 of 1995);
- Public Finance Management Act (Act 1 of 1999);
- Promotion of Access to Information Act (Act 02 of 2000);
- Protection of Personal information (POPI) Act 2013 (Act 4 of 2013);

- Protection of Information Act, 1982 (Act 84 of 1982);
- Protected Disclosure Act (Act 26 of 2000);
- Electronic Communications and Transactions Act, 2000 (Act 25 of 2000);
- Public Service Regulations, 2016, as amended; and
- Directives issued on:
  - National Minimum Information Requirements (NMIR); and
  - Guide on the functionality of Persal to promote the optimal utilisation of the system.
- Directives issued by:
  - The Department of Public Service and Administration; and
  - National Treasury.

3 DEFINITION OF TERMS

3.1 **"Approver / Revisor"** refers to the employee responsible for approving a transaction, after the transaction has been captured by the User.

3.2 **"Authoriser"** refers to the employee responsible for authorising a transaction, after the transaction has been approved by the Revisor.

3.3 **"Department"** refers to the Department of Home Affairs.

3.4 **"Exception reports"** refers to reports which are generated programmatically by the Persal system, and reflect those instances where records / transactions do not comply with the required data criteria of the Persal system.

3.5 **"Persal Controller"** refers to the employee responsible for Persal in the Department of Home Affairs.

3.6 **"Personnel Controller"** refers to the employee responsible for Human Resource functions performed on Persal.

3.7 **"Provincial Controller"** refers to the employee responsible for Human Resource and Finance functions performed on Persal, at a Provincial level.

3.8 **"Salary Controller"** refers to the employee responsible for Finance functions performed on Persal.

3.9 **"User"** refers to an employee who has been authorised to access and capture transactions on Persal.

4 PURPOSE AND SCOPE

The Policy shall apply to all authorised Users of the Persal system, individual members in Branches/Provinces within the Department who are involved with the utilization of the Persal system, and / or Persal information.

5 POLICY ROLL-OUT AND COMPLIANCE MONITORING

5.1 The roll-out of this Policy will be facilitated by the Branch: Human Resource Management and Development, applying general change management practices.

5.2 The Policy will be further accompanied by detailed standard operating procedures, with the relevant forms and checklists, to ensure uniform implementation. These procedures may be reviewed as and when necessary.

5.3 Compliance to this Policy is the responsibility of each User.

5.4 Monitoring and evaluating compliance to this Policy is the responsibility of each relevant Controller.

5.5 Compliance monitoring will also be performed by local Human Resource Management Teams responsible for the implementation of this Policy during day-to-day operations, which includes periodic audits.

5.6 An oversight function will be undertaken by the Persal Controller.

6 POLICY REVIEW AND AMENDMENT

Should there be changes in legislation, directives or guidelines affecting the functionality of Persal, and / or the implementation of new systems which will need to be taken into consideration, this Policy may be reviewed.

7 POLICY PROVISIONS

This policy provides for the:

7.1 Management of Persal User access;

7.2 Roles and responsibilities of the key role players in the management and utilisation of Persal;

7.3 Training requirements for Persal Users;

7.4 Measures to maintain Persal data integrity; and

7.5 Oversight, monitoring and evaluating the utilisation of Persal.

8 GENERAL PRINCIPLES

8.1 All Users must ensure:

- compliance with the "Persal System Policy" and related procedures;
- that she / he is subject to ongoing in-house training, self-development, and attends all formal Persal training scheduled by National Treasury;
- the optimal utilisation of the functions and capabilities of Persal; and
- that the highest levels of confidentiality of information is maintained.

8.2 All forms utilized to manage Persal access, User profiles and the administration of training must be filed by the relevant Controller in a secure location, and must be available for audit purposes.

8.3 A User is required to ensure that her / his Persal passwords are kept confidential. Where any breach in confidentiality is identified, such will be addressed through the Departmental Disciplinary Code and Procedure.

8.4 A User and / or a User's supervisor should inform the relevant Controller in writing, if the User no longer requires access to Persal.

8.5 Persal interfaces electronically with different financial systems used in Government, such as; financial institutions, pension and medical schemes. National Treasury is therefore responsible for the maintenance of Persal and enhancements, whist the daily operations on Persal is the responsibility of each User.

9 ROLE-PLAYER RESPONSIBILITIES

9.1 The effective and efficient utilisation of Persal is dependent on the following role-players: Controller (Persal, Personnel, Salary and Provincial), Revisor, Authoriser and User, who are appointed in the Department. The responsibilities of the aforementioned role-players are reflected below.

9.2 Persal Controller

9.2.1 The Persal Controller should be based at the Head Office, within the Branch: Human Resource Management and Development, and should be suitably qualified in terms of Persal experience, skill and training (formal and / or informal) to undertake this function.

9.2.2 The Persal Controller is responsible for the appointment and creation of User Id's for the:

- Personnel Controller (Based at Head Office);
- Salary Controller (Based at Head Office) and
- Provincial Controller (Based at Provincial Offices).

9.2.3 The Persal Controller is responsible for:

- regulating access and the use of Persal,
- managing the technical, system and User support, and
- facilitating formal Persal training with National Treasury, as well as informal / in house training (where required) for the Department.

9.2.4 The Persal Controller must:

- ensure professional, effective and efficient interaction between the Department and National Treasury, as well as the relevant Departmental Controllers;
- communicate Persal circulars, messages and directives to all Users in the Department, and
- attend the National Persal Forum (hosted by National Treasury), and provide feedback to the relevant stakeholders.

9.2.5 The Controller will:

- grant Persal access to a User, strictly on application;
- ensure that functions are allocated to a User;
- evaluate and recommend / reject Departmental requests for changes to Persal;
- manage the System Change Control (SCC) process on Persal,
- ensure that Persal exceptions / notifications are addressed and cleared, monitor the Persal Suspense File as well as recommended actions; and
- manage the provision and supply of information, and statistics to the relevant parties.

9.2.6 The Controller will oversee Persal control and audit measures to ensure the effective use of Persal, by way of:

- quarterly audits to review User access rights;
- monthly auditing of service terminations in order to remove User access,
- periodic audits to ensure that Persal information is accurate, comprehensive and updated;
- removal of Users who have not logged on within 2 months; and
- record keeping for audit purposes.

9.2.7 The Supervisor of the Persal Controller will oversee and verify identified activities performed by the Persal Controller. Such activities may include but are not limited to; Users created, modified, terminated and the reset of passwords.

9.2.8 The utilisation of the User Id of another User is prohibited, except when appointed, in writing, as a Relief Controller.

9.3 Personnel, Salary and Provincial Controller

9.3.1 The relevant Controller may be based at Head Office and / or Provincial Offices, and must be suitably qualified in terms of Persal experience, skill and training (formal and / or informal) to undertake this function.

9.3.2 The relevant Controller is responsible for the appointment and creation of User Id's for the:

- User (specific to HR / Finance functions);

- Reviser (approves a User's transactions); and
- Authoriser (authorises transactions with financial implications).

9.3.3 The relevant Controller must:

- ensure that Persal access is only granted on application;
- ensure that functions are allocated to a User;
- implement measures to ensure that Persal information is accurate, comprehensive and updated; manage the provision and supply of information and statistics to the relevant parties;
- facilitating formal Persal training with Provincial Treasury Departments, as well as informal / in-house training (where required) for Users in the Branch / Province; and
- ensure that Persal exceptions / notifications (as received from the Persal Controller) are addressed and cleared, and ensure that the recommended actions to clear the Persal Suspense File is implemented;
- manage the provision and supply of information, and statistics to the relevant parties; and
- manage the System Change Control (SCC) process on Persal (this is relevant only to the Salary Controller).

9.3.4 The relevant Controller is responsible for implementing control and audit measures to ensure the effective use of Persal, by way of:

- clearing of Persal exceptions;
- undertaking User account maintenance as directed by the Persal Controller;
- quarterly assessment whether the allocated Persal functions are still applicable for Users;
- monthly auditing of service terminations in order to remove User access,
- extracting reports to monitor faulty, rejected transactions and transactions awaiting approval / authorization, in respect of Users allocated within her / his control;
- monitoring the suspense and transaction files, and investigating questionable transactions, and
- record keeping for audit purposes.

9.3.5 The relevant Controller will periodically oversee and verify identified activities performed by the relevant Users.

9.3.6 The utilisation of the User Id of another User is prohibited, except when appointed, in writing, as a Relief Controller.

9.4 Persal Revisor / Authoriser

9.4.1 The Persal Revisor / Authoriser must:

- monitor all transactions performed on Persal by a User;
- consider and either approve / disapprove or authorise transactions based on the relevant source documentation;
- implement measures to ensure the updating and maintenance of the system to ensure credible and reliable information;
- extract reports to monitor faulty, rejected transactions and transactions awaiting approval / authorisation, in relation to a User allocated under her / his control; and
- promote compliance with the National Minimum Information Requirement (NMIR).

9.5 Persal User

9.5.1 A Persal User must:

- ensure that her / his Persal passwords are kept confidential and is not shared with anyone;
- instate a transaction based on the relevant source documentation, and that such source documents are duly filed for record keeping, and audit purposes;
- ensure that the data captured on Persal is accurate; and
- investigate / correct / remove exceptions which reflect on the Persal Suspense File.

10 PERSAL TRAINING

10.1 To promote a better understanding and ensure the optimal utilization of Persal, it is necessary that all Persal Users are properly trained;

10.2 The Persal / Provincial Controller will facilitate a User's nomination for training and will inform the User, upon confirmation from National / Provincial Treasury.

10.3 In-house / informal training should be undertaken, before the formal training through National / Provincial Treasury is arranged to ensure service delivery continuity, whilst the formal training is being arranged. In this regard, all Persal transactions implemented by the User must be closely monitored by the relevant supervisor.

10.4 All formal training costs will be covered by National / Provincial Treasury, since training is provided at no cost to the Department. This cost excludes hotel accommodation and subsistence and travel costs, which must be paid for by the Department, through the Departmental Travel and Subsistence Policy.

11 PERSAL DATA INTEGRITY AND CONFIDENTIALITY

11.1 All Users will be required to declare that s/he must:

11.1.1 Protect to the fullest extend required by law, all information in any format displayed or obtained from Persal;

11.1.2 Exercise and maintain the highest levels of confidentiality in the utilisation of Persal information. Such information may not be shared with any unauthorised person;

11.1.3 Never use or share information obtained from Persal in any way that is detrimental to the Government or its employees, and strictly observe all confidentiality protocols;

11.1.4 Acknowledge that the her / his computer and account is equivalent to the her / his legal signature;

11.1.5 Never disclose her / his ID or password to anyone, or allow anyone other than her / himself to access the system using that account information; and

11.1.6 Understand that s/he is responsible and accountable for all entries made and all information accessed under her / his User account, even if such action was committed by self, or by another due to the Users intentional or negligent actions.

11.2 Ensure that all data / transactions are accurately and timely captured on Persal, and source documents are duly filed for record / audit purposes.

11.3 Exception reports reflecting transactions / deviations must be promptly investigated, and cleared by the relevant functional unit (Human Resource and Finance).

11.4 The relevant Controller will monitor the progress made on the exception reports.

12 COMPLIANCE WITH NATIONAL MINIMUM INFORMATION REQUIREMENTS (NMIR)

To enable effective planning, management and policy development, the Head of Department is responsible for ensuring that all information captured and stored on Persal is accurate, credible / reliable, regularly audited, and in full compliance with the NMIR.

12.1 The NMIR prescribes that the Department is required to collect (update) and record the following information as a minimum, in respect of all employees:

12.1.1 Essential biographical information;
12.1.2 Current rank and salary information;
12.1.3 Education, training and development information;
12.1.4 Career incidents within the Public Service;
12.1.5 Disciplinary matters; and
12.1.6 Organisational and geographical information.

12.2 The Persal Controller in collaboration with the various Controllers will identify the need / frequency for the refresh of the NMIR in the Department.

13 UNATHORISED ACTIVITIES AND FRAUD RELATED TO PERSAL

13.1 All cases of suspected fraudulent / unauthorised activity must immediately be reported to the relevant Controller, for investigation in partnership with the relevant Supervisor.

13.2 Unauthorised activity comprises but is not limited to; the utilisation of another Users password, negligence in the protection of passwords, unauthorised transactions without the relevant source documents, negligence in the protection of Persal information, and sharing of information to unauthorised persons, etc.

13.3 The relevant Controller must immediately suspend the User's access to Persal and investigate the allegations / activity. Depending upon the outcome of the investigation, the User may be subject to corrective / disciplinary action, which will be undertaken in compliance with the Departmental Disciplinary Code and Procedure.

13.4 Where a User has been found guilty of unauthorised and / or fraudulent activity on Persal, the User will no longer be allowed to access Persal.