HUMAN SETTLEMENTS BRANCH

PERSAL USER ACCOUNT POLICY

"Working together we can do more"
<table>
<thead>
<tr>
<th>NO.</th>
<th>TOPIC</th>
<th>PG</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>BACKGROUND</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>PURPOSE</td>
<td>4</td>
</tr>
<tr>
<td>4.</td>
<td>OBJECTIVE</td>
<td>4</td>
</tr>
<tr>
<td>5.</td>
<td>APPLICABILITY</td>
<td>5</td>
</tr>
<tr>
<td>6.</td>
<td>DEFINITIONS AND INTERPRETATION</td>
<td>5</td>
</tr>
<tr>
<td>7.</td>
<td>AUTHORISATION</td>
<td>7</td>
</tr>
<tr>
<td>8.</td>
<td>POLICY PROVISIONS</td>
<td>8</td>
</tr>
<tr>
<td>8.1</td>
<td>Access Control</td>
<td>8</td>
</tr>
<tr>
<td>8.2</td>
<td>Disclosure of Persal Information</td>
<td>11</td>
</tr>
<tr>
<td>8.3</td>
<td>Persal Training</td>
<td>13</td>
</tr>
<tr>
<td>8.4</td>
<td>Persal related fraudulent activity</td>
<td>14</td>
</tr>
<tr>
<td>8.5</td>
<td>Compliance with National Minimum Information Requirements (NMIR)</td>
<td>15</td>
</tr>
<tr>
<td>9.</td>
<td>ROLES AND RESPONSIBILITIES</td>
<td>16</td>
</tr>
<tr>
<td>9.1</td>
<td>The duties of a User</td>
<td>16</td>
</tr>
<tr>
<td>9.2</td>
<td>The duties of the Persal Reviser/Authoriser</td>
<td>17</td>
</tr>
<tr>
<td>9.3</td>
<td>The duties of the Personnel and Salary Controller</td>
<td>18</td>
</tr>
<tr>
<td>9.4</td>
<td>The duties of the Departmental Persal Controller</td>
<td>19</td>
</tr>
<tr>
<td>9.5</td>
<td>The duties of the Departmental Persal Manager</td>
<td>21</td>
</tr>
<tr>
<td>10.</td>
<td>MONITORING, EVALUATION AND CONTROL</td>
<td>22</td>
</tr>
<tr>
<td>11.</td>
<td>IMPLEMENTATION DATE</td>
<td>22</td>
</tr>
<tr>
<td>12.</td>
<td>APPENDICES/ANNEXURES</td>
<td>23</td>
</tr>
</tbody>
</table>
NORTH WEST DEPARTMENTAL ADMINISTRATION PERSAL (PERSONNEL AND SALARY SYSTEM) USER POLICY

1. INTRODUCTION

This policy framework provides for the following:

1.1 Background;
1.2 Purpose;
1.3 Objectives;
1.4 Applicability;
1.5 Authorization;
1.6 Policy Provisions;
1.7 Roles and Responsibilities;
1.8 Monitoring and Evaluation; and implementation date of the Persal user policy in the Department Human Settlements

2. BACKGROUND

This policy was implemented and approved by PERSAL Provincial Treasury and was amended accordingly.

3. PURPOSE

The purpose of this Departmental policy is to regulate and manage the usage of the Persal system in the Departments of Human Settlements.

4. OBJECTIVE

The objective of this Departmental policy is to:

4.1 Provide guidelines to ensure PERSAL is managed and monitored effectively throughout the department;
4.2 Ensure alignment to National and Provincial Treasury PERSAL notices, directive, policies and practices;
4.3 To clearly define processes to assist in the management and prevention of fraud and corruption on the Persal system; and
4.4 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).
5. APPLICABILITY

The provisions of this policy document shall apply to all PERSAL users in the Department of Human Settlements.

6. DEFINITIONS AND INTERPRETATION

For the purpose of this policy document, meanings and definitions of the terms used in the document are provided below:

"adaptor address" means the unique network card address of a personal computer, can also be referred to as the MAC or Physical Address of a personal computer.

"authoriser" means a user responsible for authorizing transactions using function #6.8.30 after the transaction has been approved by the reviser.

"complete user ID" means the user ID allocated to a user which enables him/her access to the mainframe.

"Departmental Persal Controller" means the employee who manages the Persal Controller functions within the Department.

"Employee" is a Public Servant.

"Employer" means the State as an employer in the department.

"Exception reports" means reports which are generated programmatically by the system which reflect those instances where records or transactions do not comply with the required validations of the system.

"IP address" means a 32-bit address used to identify the adaptor address on a network.

"Key Persal functions" means a list of specific essential Persal functions identified and grouped per training course.

"PC" means a Personal Computer.

"Password" means a secret combination of letters and numbers which is linked to
the user ID.

"PERSAL" means the Personnel and Salary System.

"Persal Controller" means an employee 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, support and training to perform their duties effectively and efficiently 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 user ID allocated to a user which enables him/her access to the Persal System.

"Person" is a non-public servant (employee) appointed to perform functions/duties for the Department.

"Departmental Persal Controller" means the employee who performs the transversal Persal Controller functions within the Department.

"Relief Persal Controller" means the employee who is appointed to perform the functions assigned to the Persal Controller in his or her absence.

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

"Third party" means any person, body or organisation who is not the employer or the employee, including but not limited to financial institutions, insurance institutions, Retailers and Debtors.

"user" means any Official/Consultant who has a user ID to access the Persal system.
7. **AUTHORISATION**

The development of this Departmental policy has been undertaken by reviewing and considering the following legislation and documentation:

7.1 Constitution, 1996
7.2 Public Service Act, 1994 (Proclamation No. 103 of 1994)
7.3 Public Service Regulations, 2001
7.4 Public Finance Management Act, 1999 (Act No. 1 of 1999)
7.5 Treasury Regulations, 2005
7.6 Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
7.7 Guide on the functionality of Persal to promote the optimal utilisation of the system
7.8 National Minimum Information Requirements

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

7.9 Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997)
7.11 Employment of Educators Act, 1998 (Act No. 76 of 1998)
7.12 Financial Intelligence Act, 2001 (Act No. 38 of 2001)
7.13 Government Employees Pension Law, 1996 (Act No. 21 of 1996)
7.16 Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
7.17 Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 2 of 2002)
7.19 Unemployment Insurance Act 2001 (Act No. 63 of 2001)

And Directives issued by:

7.20 Department of Education (National)
7.21 Department of Health (National)
7.22 National Treasury
7.23 The Department of Public Service and Administration
7.24 Department of Finance: Persal Support
7.25 The South African Revenue Services
POLICY PROVISIONS

8.1 Access Control

8.1.1 The Head of Department or his or her designee in the respective Departmental Departments is responsible for appointing a Departmental Persal Controller in writing.

The employee appointed as Departmental Persal Controller must be computer literate, must have passed the Persal Controllers’ Course and have extensive knowledge of the functionality and capabilities of the Persal system. The employee should also have thorough knowledge of the Public Service Regulatory Framework and Financial Administration policies and prescripts.

8.1.2 Once appointed as a Departmental Persal Controller, it is recommended that the employee attends all Persal courses, writes and passes the examination to further improve his/her knowledge of the Persal system, thus enabling him/her to provide efficient support to his/her users.

8.1.3 The Departmental Persal Controller is responsible for the creation of Persal user ID’s for the following employees/persons subject to the completion and approval of the “Persal User Application Form” (Annexure A):

8.1.3.1 Assistant Persal Controller;
8.1.3.2 A person employed within the Public Service who is required to work on Persal, performing functions relevant to his/her duties;
8.1.3.3 An Internal Auditor, auditing personnel and/or salary administrators who require access to Persal using least privilege principle;
8.1.3.4 A person from the Office of the Auditor-General auditing personnel and salary administration who requires access to Persal using least privilege principle; and
8.1.3.5 A contract worker, consultant, casual employee or intern employed by a department who is required to work on Persal.

8.1.4 All Persal Controllers, Revisers and Users must be security vetted in terms of the Minimum Information Security Standards.

8.1.5 The “Undertaking and Acknowledgement of Liability” form (Annexure B) must be completed and signed in black ink by the user upon receipt of his/her user ID. By signing this document, the user acknowledges that he/she shall be held liable and responsible for all transactions done using his/her user ID. A copy of the “Undertaking and Acknowledgement of Liability” form must be submitted to the Department of Finance: Persal Support and the original form must be filed by the Persal Controller in a secure location.

8.1.6 A Persal Manager/Controller has the mandate to refuse access, terminate or temporarily withdraw a user’s access to the PERSAL system if:-
8.1.6.1 the user does not sign the "Undertaking and Acknowledgment of Liability" form;
8.1.6.2 a copy of the "Undertaking and Acknowledgment of Liability" form is not submitted to the Department of Finance: Persal Support;
8.1.6.3 there is suspected misuse of his/her user ID;
8.1.6.4 there is suspected fraudulent activity;
8.1.6.5 a user ID is not utilised for a period of 1 month; and
8.1.6.6 a user does not comply with the training requirement as stated in paragraphs 8.3.3 and 8.3.4.

8.1.7 A Persal Controller must appoint a Relief Persal Controller in the event of him/her being absent from work. Annexure C (Appointment of Relief Persal Controller) must be completed. A copy of the form must be submitted to the Department of Finance: Persal Support and the original form must be filed by the Persal Controller in a secure location.

8.1.8 The Persal Controller must ensure that the functions allocated to users are directly related to the user's job description. The Persal Controller and the Department of Finance: Persal Support reserves the right to restrict the usage of certain functions.

8.1.9 The "Allocation/Removal of Functions" form (Annexure D) must be completed and submitted to the Persal Controller should the user require additional functions to be allocated or removed.

8.1.10 The "Allocation/Amendment of User's Reviser" form (Annexure E) must be completed and submitted to the Persal Controller, should there be a need to change the users' reviser/s.

8.1.11 The "Allocation/Amendment of transaction codes for the Authoriser" form (Annexure F) must be completed and submitted to the Persal Controller, should there be a need to allow a user to authorise transactions.

8.1.12 For security reasons, it is recommended that each user, has his/her own computer to access the system. All user ID's must be restricted to a terminal and/or distribution unless necessary motivation as to why this is not possible is provided and approved by the Persal Manager.

8.1.13 No approval or authorization is allowed on the Persal Controller user ID. The Persal Controller should create a production ID for him/herself and that production user ID may be restricted to a terminal and/or distribution as far as its possible.

8.1.14 A user must log off each time he/she leaves the personal computer to prevent misuse of his/her Persal User ID.

8.1.15 A user is strictly prohibited from utilising the user ID of another employee/person except when
appointed as a Relief Persal Controller as in paragraph 8.1.8.

8.1.16 A “Persal/Complete User ID Reset” form (Annexure G) must be completed by the user and submitted to the Persal Controller, in order for the user ID’s password to be reset and the form must be filed in a secure location.

8.1.17 A supervisor/controller of a user must inform the Persal Controller immediately in writing if the user no longer requires access to the system by ensuring the user completes and submits the “Terminate Persal User Application Form” (Annexure H).

8.1.18 The Department of Finance: Persal Support is responsible for regulating access to the system during both normal working hours (8:00 to 16:30), after hours (16:30 to 7:00) and during weekends. The “Request to access the Persal system after official working hours” form (Annexure I) must be completed and submitted to the Department of Finance: Persal Support, should a user require access to the system during weekends or after normal working hours.

8.1.19 All forms utilised to manage access to the system, user profiles and the administration of training must be filed by the Persal Controller in a secure location.

8.2 Disclosure Of Persal Information
A user must 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 and that any person or third party does not obtain unauthorised access thereto.

8.2.1 Attending to requests for verification of employment by a third party (e.g. Financial Institutions, Insurance Institutions or Debtor), the third party must provide all the information and the user may only affirm or refute the correctness of the given information.

8.2.2 A user may not disclose any personal or other information, stored on the Persal system, regarding an employee or the employer’s organisation to any other employee, person or third party unless the employee, person or third party has the necessary authority to receive such information in terms of any relevant legislation (including, but not limited to, the Public Audit Act, 2004 (Act No. 25 of 2004) and the Income Tax Act, 1962 (Act No. 58 of 1962)), a court order or relevant departmental delegations of authority.

8.2.3 The Persal Manager or Departmental Persal Controller: can provide Persal Information to the following on written request, SARS, Departmental Internal Audit and the Auditor-General. It is necessary for the “Persal Information Request” form (Annexure J) to be completed and signed by the Persal Manager or Controller.
8.2.4 It is the responsibility of any user who has access to extract information from the Persal system in the form of a printed report, work file, electronic report or a screen print to maintain a register of the details of the information supplied and of the person who they provided the information to.

8.2.4.1 Name of requestor;
8.2.4.2 Contact telephone number of requestor;
8.2.4.3 Department or institution of requestor;
8.2.4.4 Name of person collecting the report;
8.2.4.5 Persal number of person collecting the report;
8.2.4.6 Description of information provided/collected;
8.2.4.7 Signature of person collecting the report; and
8.2.5.8 Date collected.

8.2.6 Positive identification is required prior to releasing information.
(Must be in written form by an authorized official)

8.2.7 If the information is emailed to the requestor then a copy of the email must be retained and filed.

8.3 Persal Training
In order to promote a better understanding of Persal, ensure optimal utilisation of the system and minimize errors, it is necessary to ensure that all Persal Users are properly trained. This will contribute to ensuring that Government has credible and reliable information on its employees that will in turn contribute to informed decision-making in Government.

8.3.1 A User who is required to attend a Persal training course must complete the "Training Nomination" Form (Annexure K) and submit it to the Persal Controller. The Departmental Persal Controller must ensure that all nominees comply with course prerequisites as per the nomination form. The submission of the "Training Verification" Form (Annexure L) confirms attendance of a course.

8.3.2 For the purposes of this policy key functions have been identified and grouped per training course (Annexure M reflects the key Persal Functions per course). It is compulsory for all users to attend the Persal Introductory Course and the relevant course/s should he/she be allocated particular key functions.

8.3.3 Should a learner not pass the Persal Introduction Course after three attempts, the Persal Controller or the Department of Finance: Persal Support must temporarily withdraw the user’s access to the system until such time as the user passes the examination? In exceptional circumstances, limited access can be granted until such time the user meets the requirements.
8.3.4 Should a learner not pass the relevant course examination after three attempts, the Persal Controller must temporarily withdraw the user's access and recommend that the necessary key Persal functions pertaining to the relevant course be removed. Access must be re-instated once the Persal Controller has removed the particular functions or when the learner successfully passes the examination.

8.3.5 The Persal Controller must remove access to the key Persal functions should an employee not attend the relevant courses and not pass the necessary examinations.

8.3.6 The Departmental Persal Manager/Controller reserves the right to remove a user's access to the system on a written instruction from the MEC/HOD of the Department.

8.4 Persal related fraudulent activity

8.4.1 Once fraudulent activity is suspected, the person who suspects the fraud must report it to the Departmental Persal Manager / Controller immediately.

8.4.2 The Departmental Persal Controller must temporarily withdraw access to the system from any user who may be involved in alleged fraudulent activities. The Department of Finance: Persal Support must be notified immediately of any fraudulent activity.

8.4.3 The Departmental Persal Controller must report the alleged fraudulent transaction/s immediately to the Departmental Internal Control/Audit unit for investigation.

8.4.4 The Persal Controller must ensure that all relevant Persal evidence and source documents are made readily available to the Departmental Internal Control/Audit unit, Departmental Internal Audit, Auditor General of South Africa, Office of the Premier Forensic unit or a company appointed for the investigation to be conducted.

8.4.5 The Departmental Persal Controller or Internal Control/ Audit Unit must submit progress reports regarding alleged fraudulent activities to the Department of Finance: Persal Support on a regular basis until finalisation of the investigation.

8.4.6 Once a Persal user has been found guilty of committing fraudulent activity on Persal, such user must no longer be allowed access to the system.

8.4.7 Any user, who has been found guilty of misusing the Persal system i.e. disclosing confidential Persal information to any other person, shall have disciplinary action taken against him or her.

8.5 Compliance with National Minimum Information Requirements (NMIR)
8.5.1 The NMIR prescribes that Departments are required to collect and record information in the following areas:-

8.5.1.1 Essential biographical information for all employees;
8.5.1.2 Current rank and salary information for all employees;
8.5.1.3 Education, training and development information for all employees;
8.5.1.4 Career incidents within the public service;
8.5.1.5 Disciplinary matters;
8.5.1.6 Leave;
8.5.1.7 Organisational and geographical information; and
8.5.1.8 All posts on the fixed establishment.
8.5.1.9 Equipment

8.5.2 To enable effective planning, management, and policy development, the Head of Department is responsible for ensuring that all information captured and stored on the Persal system is accurate, credible, reliable, regularly audited and complies with the National Minimum Information Requirements.

9 ROLES AND RESPONSIBILITIES

PERSAL electronically interfaces with different financial systems that are in use in Government e.g., financial institutions, pension funds and medical schemes. The normal day to day operation of the system is the responsibility of each Department while National Treasury is responsible for the maintenance of the system and enhancements. In Departmental Administrations, a PERSAL Support Office is responsible for the rendering of transversal services to the different Departments.

The effective and efficient utilisation of the Persal System is dependent on the following role players: Users, Revisers, Personnel Controller, Salary Controller, Departmental Persal Controller and the Departmental Persal Manager. The responsibilities of the aforementioned role players are reflected below.

9.1 The duties of a User are as follows:

9.1.1 Processes transactions with regard to: -
9.1.1.1 Human Resource Planning (organisation and establishment)
9.1.1.2 Personnel Administration
9.1.1.3 Salary Administration
9.1.1.4 Labour Relations
9.1.1.5 Human Resource Development

9.1.2 A user may only instate a transaction based on relevant source documentation;
9.1.3 Maintains the data captured and stored on Persal and ensure it is accurate;
9.1.4 Corrects/removes exceptions (including Persal audits) on the system; and
9.1.5 Subjects himself/herself to ongoing in-house training and self-development

9.2 The duties of the Persal Reviser/Authoriser are as follows:

9.2.1 Approves/authorises suspense file transactions in terms of local delegations and Public Service Directives and/or internal departmental policies;

9.2.2 A reviser/authoriser may only approve or authorise a transaction based on relevant source documentation;

9.2.3 Implements measures to ensure the updating and maintenance of the system to ensure credible and reliable information;

9.2.4 Promotes compliance with the National Minimum Information Requirements (NMIR);

9.2.5 Extracts reports to monitor faulty, rejected transactions and transactions awaiting approval/authorisation in respect of distributions under his/her control, on a regular basis;

9.2.6 Ensures that any exceptions reflected on the exception reports are corrected on the system; and

9.2.7 Subjects himself/herself to ongoing in-house training and self-development.

9.3 The duties of the Personnel and Salary Controller are as follows:

9.3.1 Controls access to Persal and ensures the selective allocation of functions to users in the division;

9.3.2 Registers and maintains user profiles for users and allocates specific functions in relation to their job description;

9.3.3 Links users to revisers;

9.3.4 Links authorisers to relevant transaction code/s;

9.3.5 A Personnel/Salary Controller may only amend/change a user ID profile based on relevant source documentation;

9.3.6 Monitors and encourages interaction between the users and revisers;

9.3.7 Accounts for effective utilisation of the Persal System in the Department;

9.3.8 Identifies and implements Persal control and audit measures;

9.3.9 Ensures that procedure manuals are properly compiled and updated and monitors the implementation thereof;

9.3.10 Ensures that the Revisers/Authorisers extract reports to monitor faulty, rejected transactions and transactions awaiting approval/authorisation in respect of distributions under his/her control, on a daily basis;

9.3.11 Monitors the transactions on the suspense and transaction files and follows up questionable transactions;

9.3.12 Ensures that exceptions (including Persal audits) are verified, investigated and that corrective action is taken at all times;

9.3.13 Manages information including monitoring and data compliance;
Manages the provision of information and statistics to appropriate parties;
Evaluates and recommends changes to the system in line with Departmental policies/procedures to the Departmental Persal Controller;
Interacts with the BAS Controller to ensure that a reconciliation between BAS and Persal is done on a monthly basis;
Subjects himself/herself to ongoing in-house training and self development.

9.4 The duties of the Departmental Persal Manager are as follows:

9.4.1 Monitors and ensures the effective use of the Persal system in the department;
9.4.2 Controls access to Persal and ensures the selective allocation of functions to users in the department;
9.4.3 Assesses and records the Persal training needs of the Department in conjunction with section heads, in order to make nominations for training courses, as and when required;
9.4.4 Responsible for the creation and maintenance of departmental codes on the departmental code file;
9.4.5 Evaluates and recommends/rejects requested changes to the Persal system to the Departmental Persal Controller;
9.4.6 Manages and controls Persal circulars and messages and brings important issues to the attention of all users in the Department;
9.4.7 Ensures professional, effective and efficient interaction between the Persal User Support and the Departmental Departments;
9.4.8 Responsible for the composition and maintenance of departmental manuals and procedures;
9.4.9 Act as Persal advisor in their department;
9.4.10 Implements Persal control and audit measures;
9.4.11 Provides continuous support, guidance and training to all Persal role players within the Department; and
9.4.12 Subjects him/herself to ongoing in-house training and self-development.

9.5 The duties of the Departmental PERSAL Controller are as follows:

9.5.1 Overall managerial responsibility for the technical, system support, user support and Persal training in the Province;
9.5.2 Controls access to Persal and ensures the selective allocation of functions to users in the Province;
9.5.3 The Departmental Persal Controller may only amend/change a user ID profile of a Departmental Persal Controller based on relevant source documentation;
9.5.4 Responsible for the orientation of all users of the system;
9.5.5 Responsible for the creation and maintenance of codes on the departmental code file;
9.5.6 Manages and controls Persal circulars and messages and brings important issues to the attention of all users in the Province;