



Approval Date	20 -07 -2023
Periodical Review	3-year basis
Commencement Date	20 - 07 - 2023
Review Date	20 - 07 - 2026

**STANDARD OPERATING PROCEDURE: MODIFY BAS SYSTEM USER ACCOUNT**

<b>TITLE OF SOP</b>	MODIFY BAS SYSTEM USER ACCOUNT
<b>SOP Number</b>	FSA-BAS-02
<b>Purpose</b>	The purpose of this SOP is to define and outline the roles and responsibilities of the various BAS role-players and provide standard guidelines regarding management, access, and usage of the BAS in Eastern Cape Department of Social Development.
<b>Scope</b>	This SOP is applicable to all users of the BAS accounting system in all provincial departments in the Eastern Cape Province.

<p><b>Definitions and Acronyms</b></p>	<p><b>BAS:</b> Basic Accounting System</p> <p><b>Departmental code file:</b> Codes that are unique to the specific department</p> <p><b>System Controller:</b> An employee who is responsible for registering and maintaining user profiles of users under his/her control, and also ensures that users are equipped with the required tools, support and training to perform their duties effectively and efficiently on the System.</p> <p><b>Departmental Parameters:</b> Departmental Parameters contain values that are specific to the department which are maintained by the department's System Controller. The department has a choice to alter these parameters according to its own needs</p> <p><b>Function:</b> The task that is allocated to the user</p> <p><b>Group Profiles:</b> A group of users based on a common function that a user requires ID: A unique code allocated to a user in order to access the system(s)</p> <p><b>Over Expenditure Authorizers / Supervisors:</b> A user who is responsible for overriding budget block</p> <p><b>POC:</b> Period Open and Close journals that are affected at final year end closure of BAS system, with the authorization from the Auditor General's office.</p> <p><b>SCoA:</b> Standard Chart of Accounts; this is a chart with the list of all Accounts used within Government as a whole</p> <p><b>Suspense Control Accounts:</b> System control accounts, which must have zero balances at month and year-end closure</p> <p><b>Suspense File Transaction:</b> A transaction that has the status of awaiting approval/ authorization or disapproval/rejection</p> <p><b>Transversal Systems:</b> BAS, PERSAL and LOGIS</p> <p><b>User:</b> An employee/person who applied or has a user ID to access the BAS system</p> <p><b>User Profiles:</b> The level of access required by a user</p>
<p><b>Performance Indicator</b></p>	<p>Number of credible Financial Statements</p>

**STEP BY STEP GUIDE  
MODIFY BAS USER ACCOUNT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
1.	<b>Request access</b>	<ul style="list-style-type: none"> <li>• Print BAS new user application or termination of user form from Knowledge Hub/ request the form from the office through the e-mail.</li> <li>• Supervisor indicate the user function and profile to be modified and sign.</li> <li>• Submit duly completed signed form by all relevant parties to BAS system support office.</li> </ul>	User	1 Day	<ul style="list-style-type: none"> <li>• Copy of ID (where applicable)</li> <li>• User PERSAL printout (where applicable)</li> <li>• Modification request form</li> <li>• Motivation for modification</li> <li>• Promotion/transfer letter (if applicable)</li> <li>• Acting appointment letter</li> <li>• Completed signed BAS modification request reform</li> </ul>	Create modification as requested by the end-user on BAS within 30 minutes
2.	<b>Analyze user request</b>	<ul style="list-style-type: none"> <li>• Verify the received request form if it is captured correctly and also if all the required documents are attached.</li> <li>• Verify if the user requested the relevant modification type:               <ul style="list-style-type: none"> <li>○ User profile</li> <li>○ User function</li> </ul> </li> <li>• Determine the user requested function to grant access               <ul style="list-style-type: none"> <li>○ Budget maintenance</li> <li>○ Debt maintenance</li> <li>○ Journal processing</li> <li>○ Entity maintenance</li> <li>○ Payments</li> <li>○ Online enquires and reports</li> <li>○ Receipt</li> </ul> </li> </ul>	BAS Systems Controller	30 minutes	<ul style="list-style-type: none"> <li>• Completed signed BAS user modification form</li> <li>• Signed analyzed user modification form with date.</li> </ul>	
3.	<b>Modify user account</b>	<ul style="list-style-type: none"> <li>• Login to BAS</li> <li>• Create unique user identification (Persal No) to identify the user and link it to the action or function</li> <li>• Standardize the user ID for consultants to use 8 digits of the R.S.A I. D number and for foreigner to use 8 digits of the passport number.</li> <li>• Assign the relevant user to the relevant workflow group:               <ul style="list-style-type: none"> <li>○ Budget Management</li> </ul> </li> </ul>	BAS Systems Controller	30 minutes	<ul style="list-style-type: none"> <li>• Signed analyzed user modification form with date</li> <li>• Copy of ID</li> <li>• System generated report user profile</li> </ul>	

**STEP BY STEP GUIDE  
MODIFY BAS USER ACCOUNT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
		<ul style="list-style-type: none"> <li>○ Debt maintenance</li> <li>○ Journal processing</li> <li>○ Entity maintenance</li> <li>○ Payments</li> <li>○ Receipt</li> <li>○ Enquiry and reports</li> <li>● Standardize password control in compliance with National Treasury, BAS notice 5 of 2010 to password length of at least (8) characters and must consists of a combination of numeric and alphabetical characters.</li> </ul> <p>Standardize password expiry in compliance with National Treasury, BAS notice 5 of 2010 to password expiry period be not more than 30 days.</p>				
4.	<b>Notify the user and administer the form</b>	<ul style="list-style-type: none"> <li>● Issue a written statement to the user explaining the access rights.</li> <li>● User sign the statement indicating the understanding of the conditions under which access is granted.</li> <li>● Inform the applicant about the modification telephonically that he has 30 minutes to create individual password.</li> <li>● If this period lapses the BAS system will automatically deactivate the user online enquires and reports.</li> <li>● Complete and sign "for office use" fields.</li> <li>● File the reset request form.</li> </ul>	BAS System controller	1 day	<ul style="list-style-type: none"> <li>● System generated report user profile</li> <li>● Written Statement</li> <li>● Signed written statement</li> <li>● Filed signed-off BAS user modification request forms</li> </ul>	
5.	<b>Monitor user modification on BAS</b>	<ul style="list-style-type: none"> <li>● Develop monitoring report and submit the Director: Financial Systems and Accounting Services quarterly that indicates the following: <ul style="list-style-type: none"> <li>✓ Provide the Provincial Treasury with a certificate of compliance to indicate that all users who have been appointed or seconded to other section/directorate/unit/profiles have been amended to reflect the new office of employment on the BAS system quarterly.</li> </ul> </li> </ul>	BAS System Controller	2 days	<ul style="list-style-type: none"> <li>● System generated report user profile</li> <li>● BAS modified account monitoring report</li> </ul>	

**PROCESS RISKS**

Risk Name	Risk Description	Probability (H / M / L)	Impact (H / M / L)	Control Description	System / Manual
<b>Password Sharing between users</b>	When one user shares password information with another user can lead to compromise of confidentiality, integrity and authenticity.	L	M	<ul style="list-style-type: none"> <li>• Include instructions of password maintenance on creation and reset form by BAS System controller.</li> <li>• ICT security awareness session by BAS Systems controller.</li> <li>• Amend user modification form to enhance security measures by BAS Systems controller.</li> </ul>	Manual

**REFERENCES (LEGISLATION, POLICIES, PROCEDURES, LEGISLATION & OTHER DOCUMENTATION (i.e. SOPs)**

Document Name	Section Description or Document Description
<p><b>PFMA Section 38(1)(a)(i)</b></p>	<p>PFMA Section 38(1)(a)(i) states that The Accounting Officer must ensure that the department, trading entity or constitutional institution has and maintains effective and transparent systems of financial and risk management and internal control.</p> <p>PFMA Section 38(1)(b) states that the Accounting Officer is responsible for the effective, efficient, economical and transparent use of the resources of the department, trading entity or constitutional institution.</p> <p>PFMA Section 40(1)(a) states that the Accounting Officer must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards.</p>
<p><b>DSD Privacy Policy 2021</b></p>	<p>To protect Department of Social Development from the compicance risks associated with the protection of personal information which includes:</p> <p><b>Breach of confidentiality.</b> For instance, Department of Social Development could suffer loss in credibility and trustworthy where it is found that the personal information of data subjects has been shared or disclosed inappropriately.</p> <p><b>Failing to offer choice.</b> For instance, all data subjects should be free to choose how and for what purpose Department of Social Development uses information relating to them.</p> <p><b>Reputational damage .</b> For instance, Department of Social Development could suffer a reputational damage following an adverse event such as a computer hacher deleting the personal information held by Department of Social Development.</p>
<p><b>Protection of Personal Information (Act no.04 of 2013)</b></p>	<p>Section 9 Lawfulness of processing states that (1) Personal information must be processed (a) lawfully; and (b) in a reasonable manner that does not infringe the privacy of the data subject.</p> <p>Section 10 states that Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.</p> <p>Section 11 states that Personal information must be collected directly from the data subject, except as otherwise provided for in subsection (2).</p> <p>Section 16. (1) states that a responsible party must take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.</p> <p>(2) In taking the steps referred to in subsection (1), the responsibility party must have regard to the purpose for which personal information is collected or further processed.</p> <p>Section 19. (1) states that a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent - a) loss of, damage to or unauthorised destruction of personal information;</p> <p>Bias legitimate</p>

Document Name	Section Description or Document Description
	<p>Section 24 States the following:</p> <ol style="list-style-type: none"> <li>1. A data subject may, in the prescribed manner, request a responsible party to— <ol style="list-style-type: none"> <li>a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or</li> <li>b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of section 14.</li> </ol> </li> <li>2. On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable— <ol style="list-style-type: none"> <li>a) correct the information;</li> <li>b) destroy or delete the information;</li> <li>c) provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or</li> <li>d) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.</li> </ol> </li> <li>3. If the responsible party has taken steps under subsection (2) that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.</li> <li>4. The responsible party must notify a data subject, who has made a request in terms of subsection (1), of the action taken as a result of the request.</li> </ol> <p>The responsible party must restrict processing of personal information if—</p> <ol style="list-style-type: none"> <li>(a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;</li> <li>(b) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;</li> <li>(c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or</li> <li>(d) the data subject requests to transmit the personal data into another automated processing system.</li> </ol>
<p><b>Provincial Basic Accounting System Policy 2013</b></p>	<p>To define and clarify roles and responsibilities of the various BAS role players and provide standard guidelines regarding management, access and usage of the BAS in the Eastern Cape provincial departments. The appropriate implementation and use of BAS in the province is critical to ensure that;</p> <ul style="list-style-type: none"> <li>• The system is not accessed by unauthorized persons (confidentiality).</li> <li>• Information on BAS is not altered by unauthorized persons in a way that is not detectable by authorized persons users (integrity).</li> <li>• Users of BAS are the persons who they claim to be (authentication).</li> </ul>

**AUTHORISATIONS**

Designation:	Name:	Comments:	Signature:	Date:
Director: Financial Systems and Accounting Services	M.Jaceni			30/06/2023
Recommended by: Acting CIO -	M.E.Gazi	Recommended		
Chief Financial Officer	N.S.Tutani SN	Recommended		10 July 2023
Recommended by: DDG	<del>Dr.N.Z.G.Yokwana</del> Ganca F.Z.			12/07/2023
Approved by: Head of the Department	M. Machelamba	Approved		20/07/2023
Distribution and Use of SOP	All Departmental staff			

MA