



Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

BAS PROCEDURE MANUAL

Physical Address	Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Local Government and Traditional Affairs Private Bag X0035 Bhisho 5605
Document Number	1
Document Name	BAS Procedure Manual
Contact Person	M. Njomba
Designation	Director- Budget Planning and Management
Component	Budget Planning and Management
Telephone No.	040 609 5409/ 040 609 5432
Fax No.	040 635 0165
E-mail Address	mthunzi.njomba@eccogta.gov.za/ dumisani.ndlovu@eccogta.gov.za
Date Completed	29 January 2014
Date of Approval	
Date Last Amended	July 2016
Date For Next Review	As and when necessary
Related Policies	BAS Policy

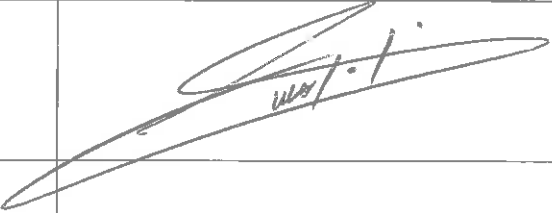
SIGN OFF

Head of Department

This BAS Procedure Manual has been recommended by Mr M.E.Baza in my capacity as Acting Head of Department of the Department of Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Procedure Manual.

The development of the Procedure Manual will ensure that the department is able to exercise its powers in compliance with the laws and regulations and also ensure the improvement of internal controls.

Signed	
Designation	Acting Head of Department
Date	05/09/2017

Executive Authority

The Department of Cooperative Governance and Traditional Affairs has unprecedented opportunity to improve the livelihood of the people by effectively rendering the many services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to challenges of its people.

I therefore trust that guidance from this Procedure Manual will contribute to the effective guidance of staff members with regards to BAS related matters.


Signed	
Designation	MEC: Honourable F.D. Xasa of Cooperative Governance and Traditional Affairs
Date	05/09/2017

TABLE OF CONTENT

1.	DEFINITIONS.....	6
2.	PURPOSE	9
3.	CREATING A NEW SYSTEM CONTROLLER USER ID.....	9
4.	PROVISION OF ACCESS TO THE ASSISTANT SYSTEM CONTROLLER	9
5.	CREATING NEW USERS/ GROUP PROFILE	10
6.	AMENDING USERS/ GROUP PROFILE	11
7.	RESETTING USER PASSWORDS.....	11
8.	DEACTIVATING/ TERMINATING USER PROFILES	12
9.	ACCESS VIOLATIONS	13
10.	CONTROLS ON ALLOCATION OF PASSWORDS.....	14
11.	CREATION OF CODE STRUCTURE	15
12.	MAINTENANCE OF DEPARTMENTAL PARAMETERS	15
13.	ORIENTATION AND TRAINING OF USERS	15
14.	GENERAL CONTROLS	16
14.1	PASSWORDS	16
14.2	UNATTENDED USER EQUIPMENT	16
14.3	MONITORING OF ACCESS AND USER ACTIVITIES.....	17
14.4	ISOLATION OF RESPONSIBILITIES	17
14.5	APPLICATION OF PROCESSING CHECKS AND VERIFICATION PROCEDURES	17
14.6	PERIODIC CHECKS AND TESTING OF CONTROLS ON THE SYSTEM.....	18
15.	MONITORING AND EVALUATION OF THE MANUAL.....	18
16.	NON-COMPLIANCE.....	18
17.	COMMUNICATION/EDUCATION OF THE MANUAL.....	19
18.	REVIEW OF THE MANUAL.....	19
19.	DATE OF EFFECT AND APPROVAL.....	19
20.	VERSION CONTROL AND CHANGE HISTORY.....	20



1. DEFINITIONS

Terms and definitions that will be used throughout the manual that need clarification for the reader can also include any keywords, technical terms and abbreviations that may be used in this document.

Word/Terminology	Definitions
BAS	Basic Accounting System
Authorizer	The User responsible for approving transactions
BAS Releases	Enhancements on BAS
Batch Run	Applications that update data on the system
Departmental Code Profile	Codes that are unique to a specific department
Departmental Parameters	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 it's own needs
Function	The task that is allocated to the user
Group Profile	A group of users based on common functions that users require
System Owner	The Senior Manager responsible for Basic Accounting System
System Controller ID	The main user ID allocated to a department for controlling and managing BAS
ID	A unique code allocated to a user in order to access the system
Interface Exceptions	Interface transaction that does not comply with BAS specifications
Over Expenditure Authorizer	A user who is responsible for authorizing the



Word/Terminology	Definitions
	over-expenditure
POC	Period open and close journals that are effected at final year end closure, with authorization from the Auditor General's office
SCoA	Standard Chart of Accounts; this is a chart with all the accounts used in Government
Source System	An external computerized system, which provides the source data to BAS
Link Codes	Codes used for transferring information from Persal into BAS
System Controller	An employee who is responsible for registering and maintaining user profiles, and also ensures that users are equipped with the required tools, support and training to perform their duties effectively and efficiently on the system.
Assistant System Controller	The individual who is registered with National Treasury as an assistant / relief System Controller
Transversal Systems	BAS, PERSAL and LOGIS
User	An employee who has a user ID to access BAS
User Profile	The level of access required by a user
CFO	Chief Financial Officer
HR	Human Resources
MEC	Member of Executive Committee
PFMA	Public Finance Management Act
NT	National Treasury
PPT	Provincial Planning and Treasury

Word/Terminology	Definitions
BAS Creation Form	A form used when creating Users
BAS Profile Change Form	A form used when changing User's access
BAS Reset Form	A form used when resetting a User's password
Syscon Reset	A form used when resetting System Controller/ Relief System Controller

PSA

2. PURPOSE

- a) To provide guidance on the effective and efficient use of the BAS system.
- b) To ensure that BAS procedures are understood and practiced by all relevant employees within the department according to prescripts.
- c) To ensure that security is improved on the system in order to safeguard the system and the system information.

3. CREATING A NEW SYSTEM CONTROLLER USER ID

- a) The CFO must send a letter, accompanied by the form containing details of the System Controller to NT requesting the new System Controller ID to be created.
- b) Upon creation of the new System Controller ID the System Controller will have to login and change the password to a self-chosen one.

4. PROVISION OF ACCESS TO THE ASSISTANT SYSTEM CONTROLLER

- a) The nominated/ appointed Assistant System Controller must be registered with NT
- b) In the absence of the System Controller the Assistant System Controller must revoke the System Controller ID on instruction by the authorized person.
- c) If Assistant System Controller has another User ID for transacting on the system, that User ID must also be revoked (refer to, BAS Policy Sec 8c (xxii))
- d) Assistant System Controller must log a call with NT for the System Controller ID reset.
- e) Assistant System Controller must email or fax the reset form with the call number to NT and copy PT.



- f) Upon reset the Assistant System Controller must login and change the System Controller ID password.
- g) When the System Controller is back in the office the same procedure explained above must be followed by the System Controller.

5. CREATING NEW USERS/ GROUP PROFILE

- a) System Controller receives a request for the creation of a user ID from the end-user's supervisor.
- b) Provincial Treasury and employees from components outside Finance and Supply Chain must write a formal request to the Department (addressed to CFO, System Owner and System Controller) requesting creation of their users.
- c) On the memorandum the supervisor must clearly state the functions that will be performed by the user and how this will not affect the segregation of duties.
- d) System Controller issues a BAS user creation form to the end user.
- e) End user submits a supervisor approved form and a copy of South African Identity Document (SA ID) to System Controller.
- f) System Controller checks the form for completeness and accuracy.
- g) System Controller rejects the request if it does not meet the assertions on (d) and send the form back to the end user.
- h) System Controller approves the request if the assertions on (d) have been met.
- i) System Controller writes to DGITO requesting BAS installation for the new User
- j) System Controller creates the new user on the system.
- k) System Controller informs the end user in writing that they have been created detailing the User ID and default password.



- l) End user log's in and change the default password to a self-chosen one which must be done within thirty (30) minutes of the user id creation.
- m) System Controller files the BAS user id creation documents.
- n) Logis integration users must be created by Logis Sytem Controller.
- o) Logis System Controller must then send a memorandum to BAS System Controller requesting the new user to be added on BAS for interface purposes.

6. AMENDING USERS/ GROUP PROFILE

- a) System Controller receives a request for the amendment of a user profile from the end-user.
- b) System Controller issues a BAS profile amendment form to the end user.
- c) End user submits a Senior Manager approved form and SA ID copy to System Controller.
- d) System Controller checks the form for completeness and accuracy.
- e) System Controller rejects the request if it does not meet the assertions on (d) and send the form back to the end user.
- f) System Controller approves the request if the assertions on (d) have been met.
- g) System Controller amends the user profile on the system.
- h) System Controller informs the end user in writing that the amendment has been made.
- i) System Controller files the user amendment documents.

7. RESETTNG USER PASSWORDS

- a) System Controller receives a request for a password reset.



- b) System Controller issues a BAS password reset form.
- c) End user submits a supervisor approved form and ID copy to System Controller.
- d) System Controller checks the form for completeness and accuracy.
- e) System Controller rejects the request if it does not meet the assertions on (d) and send the form back to the end user.
- f) System Controller approves the request if the assertions on (d) have been met.
- g) System Controller resets the password on the system.
- h) System Controller informs the end user in writing that the password reset has been done.
- i) System Controller files the password reset documents.

8. DEACTIVATING/ TERMINATING USER PROFILES

- a) BAS will automatically deactivate the user id that has not been used for more than thirty (30) days.
- b) To activate the user id a reset process explained on number 7 above will have to be followed.
- c) System Controller also checks the user activity monthly by requesting the User activity report.
- d) System Controller investigates the reasons for inactivity.
- e) Based on the findings the System Controller will terminate user(s) who have been inactive for three consecutive months.
- f) System Controller requests a PERSAL termination and transfer report and remove BAS users that appear on these reports.



- g) System Controller receives resignation or transfer letters from supervisors for all users who have resigned in a specific month and remove such users on the system before the 7th of the subsequent month.
- h) For Logis integration users, Logis System Controller must send a list of all users who have been removed from Logis to BAS System Controller every month.
- i) System Controller files all the documents for record keeping and auditing purposes.
- j) System Controller must report to the Senior Manager Budget Planning and Management on terminations on a monthly basis.

9. ACCESS VIOLATIONS

- a) Users must report access violations to the System Controller immediately as they suspect or become aware of it.
- b) System Controller must report violation of his User ID to System Owner, CFO, Provincial Treasury and National Treasury
- c) The User and Supervisor must inform the System Controller when they intend taking extended leave (maternity, long vacation etc.) to prevent any violation.
- d) Users who take leave for seven days or more must be deactivated by the System Controller.
- e) Users who are on maternity leave must be deactivated by the System Controller
- f) Requests to report to work whilst the User is on leave must be done in writing.
- g) The System Controller must investigate by requesting the user activity report to verify the workstation where access was violated.
- h) The System Controller must inform the System Owner about the reported violation and finding thereof



- i) Based on the findings the User(s) who has violated BAS access will be deactivated from BAS
- j) The System Controller will write a report to the System Owner and the CFO and document all supporting information relating to the violation.

In an event that a User has been found to be on the wrong, disciplinary processes will be instituted.

10. CONTROLS ON ALLOCATION OF PASSWORDS

- a) Users must keep their BAS passwords confidential.
- b) Users must maintain their own passwords.
- c) Passwords should never be stored on computer systems in an unprotected form.
- d) The password must be unique to the individual.
- e) The password must be at least 8 characters.
- f) The password must be different from at least five (5) previous passwords.
- g) The password must contain characters from three (3) of the following four (4) classes, but in no specific order:
 - Uppercase
 - Lowercase
 - Numerals
 - Special characters



11. CREATION OF CODE STRUCTURE

- a) System Controller receives an approved organogram from HR.
- b) System Controller creates the structure on the working document in preparation for creating responsibilities on the system.
- c) System Controller submits to Senior Manager and CFO for verification and approval.
- d) On approval System Controller creates the structure on BAS.
- e) System Controller requests a structure maintenance report and hand in to Senior Manager for verification and approval.
- f) System Controller sends the structure maintenance report to PERSAL Controller for creation of link codes and the new structure must be sent to the users.

12. MAINTENANCE OF DEPARTMENTAL PARAMETERS

- a) System Controller should amend the departmental Parameters on instruction from NT, PPT or the department.

;

13. ORIENTATION AND TRAINING OF USERS

- a) System Controller must orientate all new BAS users on the login procedures.
- b) System Controller receives training requests from the various supervisors.
- c) System Controller issues a training nomination form to the users to complete.
- d) System Controller receives a completed and supervisor approved nomination form from the users.



- e) System Controller compiles a list of users who need training for various functional areas.
- f) Users are sent to PPT for the formal training based on the schedule issued by PPT.
- g) System Controller conducts informal training on assessment of need or on request.
- h) System Controller reports to Senior Manager on all users trained on a monthly basis and provide training supporting documents.

14. GENERAL CONTROLS

14.1 Passwords

BAS user must compose passwords that are:

- a) easy to remember.
- b) not based on names, telephone numbers, dates of birth, etc.
- c) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries).
- d) free of consecutive, identical, all-numeric or all alphabetic characters.

14.2 Unattended User Equipment

BAS users must:

- a) terminate active sessions when finished, unless such sessions can be secured by an automated locking mechanism, e.g. password-protected screen saver.
- b) log computers off at the end of the session (i.e. it is not sufficient to only switch off the computer screen or terminal).



- c) secure computers from unauthorized use by means of a key lock or an equivalent control e.g. password access when not in use.

14.3 Monitoring of Access and User Activities

- a) System Controller checks the user activity monthly by using the User activity report.
- b) System Controller requests a disbursement report to check the authorizers that processed the payments after each disbursement.

14.4 Isolation of Responsibilities

- a) System Controller is not allowed to transact on the system.
- b) The system will not allow users to be a capturer and an authoriser in one functional area.
- c) The transactions will be entered onto the system by capturers,
- d) The supervisor will verify the transaction and then either reject/ authorise the transaction.
- e) If the transaction is rejected it must then go back to the capturer for correction.

14.5 Application of processing Checks and Verification Procedures

- a) The capturer must check if all the supporting documents have been furnished for each transaction.
- b) Capturer checks if the documents have been signed by authorised signatures
- c) Capturer checks if all the allocations are correct if not the transaction must not be captured.



- d) If documents are correct the transaction will then be captured on the system.
- e) Supervisor must check what is on the system against the supporting documents.
- f) Supervisor rejects the transaction if not captured correctly or sufficient documentation is not provided
- g) Supervisor authorises the transaction if the information is captured correctly and necessary documentation is attached.

14.6 Periodic Checks and Testing of the Controls on the System

- a) System Controller requests a user activity report on a monthly basis checks to keep track of what users do on the system.
- b) System Controller conducts access reviews quarterly to verify that users are still performing the roles as defined on their first access application.
- c) System Controller investigates if there are any violation from the initial application
- d) Based on the findings the System Controller may terminate or suspend access after consultation with the relevant Supervisors
- e) Internal Auditors will also request User Ids from time to time in order to test the functionality of the system and also test the controls that have been implemented.

15. MONITORING AND EVALUATION OF THE MANUAL

- a) Senior Manager Budget Planning and Management must vigorously monitor the implementation of this manual and shall submit a report to the Chief Financial Officer.

16. NON-COMPLIANCE

- a) Where the Senior Manager: Budget Planning and Management, the System
- Page 18 of 20



Controller, the Assistant Controller, and the Users are found to have infringed on the requirements of this manual, disciplinary action shall be considered in accordance with the Code of Conduct.

- b) The Head of Department or the delegated Official must ensure that the disciplinary action is taken within a reasonable period after an incident has been reported.

17. COMMUNICATION/EDUCATION OF THE MANUAL

- a) The BAS Procedure Manual must be communicated to all the users of the BAS System through workgroup contact sessions and workshops.

18. REVIEW OF THE MANUAL

- a) This manual shall be reviewed as and when necessary from the date of approval and when there are changes in the enabling legislation.

19. DATE OF EFFECT AND APPROVAL

- a) BAS Manual is the official document of the Department of Cooperative Governance and Traditional Affairs recommended by the Superintendent General and approved by the Executing Authority and shall become official from the date of it is signed.

A handwritten signature in black ink, appearing to be 'EBA', is located to the right of the text in section 19.

20. VERSION CONTROL AND CHANGE HISTORY

VERSION CONTROL	EFFECTIVE DATE	APPROVED BY	AMMENDMENT
Start from	YYMMDD (The date the policy takes effect)	Full name &Title	
2014	2014/03/31	(MEC)	
2015			
2016		(MEC)	Section 4c Section 5c,e,i Section 6c Section 7c Section 8g,h Section 9
2017			Section 5b,c,n,o Section 18a

