



Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

BAS POLICY

Departmental Contact Details	
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 Policy
Contact Person	M. Njomba
Designation	Director- Budget Planning and Management
Component	Budget Planning and Management
Telephone No.	040 609 5409
Cell Phone No.	
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	

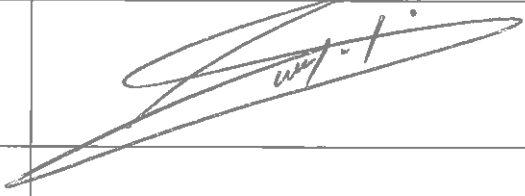
SIGN OFF

1. Head of Department

This BAS Policy has been approved 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 Policy.

The development of the BAS Policy will ensure effective and efficient management of BAS within the department.

Signed	
Designation	Acting Head of Department
Date	05/9/2017

Executive Authority

The Department of Cooperative Governance and Traditional Affairs has unprecedented opportunity to improve the live hoods 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 BAS Policy will contribute to the effective usage of the BAS system in order to improve on reporting.


Signed	
Designation	MEC: Honourable F.D. Xasa of Cooperative Governance and Traditional Affairs
Date	08/09/2017

TABLE OF CONTENT

1.	DEFINITIONS	7
2.	PREAMBLE	9
3.	PURPOSE OF POLICY	9
4.	SCOPE OF APPLICATION	10
5.	LEGISLATIVE FRAMEWORK.....	10
6.	POLICY PRINCIPLES INHERENT IN THE BAS POLICY	10
7.	OVERVIEW OF BAS	10
8.	ROLES AND RESPONSIBILITIES	11
9.	USER ACCOUNT BAS MANAGEMENT	13
10.	ACCESS VIOLATIONS	14
11.	CREATION/AMENDMENT OF CODE STRUCTURE.....	14
12.	MAINTENANCE OF DEPARTMENTAL PARAMETERS	14
13.	ORIENTATION AND TRAINING.....	14
15.	IMPLEMENTATION.....	15
16.	NON-COMPLIANCE.....	15
17.	MONITORING AND EVALUATION OF THE IMPLEMENTATION	15
18.	COMMUNICATION / EDUCATION OF THE POLICY	15
19.	DISPUTE RESOLUTION MECHANISM	15
20.	APPROVAL OF THE POLICY	16
21.	REVIEW OF THE POLICY	16

1. DEFINITIONS

Terms and definitions that will be used throughout the policy 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 (with examples if required)
BAS	Basic Accounting System
Authoriser	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
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
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
Suspense Control Accounts	System control accounts, which must have zero balance at month and year-end closure
AO	Accounting Officer
Suspense File Transaction	A transaction that has the status of awaiting authorization or rejection

Word/Terminology	Definitions (with examples if required)
System Owner	The Senior Manager responsible for Basic Accounting System
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.
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
PPT	Provincial Planning and Treasury Provincial Planning and Treasury
PFMA	Public Finance Management Act
MEC	Member of Executive Council
CFO	Chief Financial Officer
NT	National Treasury

2. PREAMBLE

Section 38(1)(a)(i) and section 40(1)(a) of the Public Finance Management Act (PFMA), Act (1) of 1999 (as amended by Act 29 of 1999):

- I. places onus on the Accounting Officer (AO) to ensure that there is an effective and transparent systems for financial management, risk management and internal controls and,
 - II. he or she must keep full and proper records of financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards.
- a) Basic Accounting System (BAS) is one of the three transversal financial systems used by government for financial control that is provided by National Treasury which ensures realisation of the requirements stated in 2(i) and (ii) above.
 - b) The normal day-to-day operation of BAS (Structures, user access, exception reports etc.) is the responsibility of each department and must be executed by the departmental System Controller.
 - c) Previous assessments and reviews by Provincial Planning and Treasury (PPT) and Auditor General have highlighted a lack of effective management (Weak system controls) of transversal system (BAS) for the department.
 - d) In order to address the concerns on (c) above the department together with Provincial Planning and Treasury (PPT) will utilize training interventions, system circulars, user forums and workshops to emphasise the importance of executing the functions in accordance with prescribed policy and procedure manual.

3. PURPOSE OF POLICY

- a) The purpose of this policy is to outline the roles and responsibilities of the various BAS role-players and provide standard guidelines regarding management, access and usage of BAS in the Department of Cooperative Governance and Traditional Affairs (COGTA).
- b) The appropriate implementation and use of the system is critical to ensure that;
 - I. The system is accessed by authorized persons (**confidentiality**)
 - II. Information on BAS is not altered by unauthorized persons in a way that it is not detectable by authorized users (**integrity**)
 - III. BAS users are the persons they claim to be (**authentication**)



- IV. The BAS system resources are safeguarded.
- V. The functions of BAS users are outlined.
- VI. The security control measures are provided to avoid misuse.

4. SCOPE OF APPLICATION

- a) This policy is applicable to all BAS users (day to day users and oversight structures) within the Department of Cooperative Governance and Traditional Affairs.

5. LEGISLATIVE FRAMEWORK

- a) This policy document aims to provide a framework within the guiding principles of the following:
 - I. PFMA
 - II. Treasury Regulations
 - III. BAS Notices
 - IV. Treasury Policy and Circulars

6. POLICY PRINCIPLES INHERENT IN THE BAS POLICY

- a) Confidentiality
- b) Integrity
- c) Authentication

7. OVERVIEW OF BAS

- a) To successfully implement and maintain BAS in the department one (1) System Controller must be appointed
- b) It is essential that the System Controller has sound knowledge of the departmental processes, procedures and departmental reporting requirements.
- c) The System Controller must undergo formal training within 12 months of his/her appointment and must pass the assessments in all functional areas currently available on BAS.
- d) The Department may appoint Assistant System Controllers who will report to the main System Controller.
- e) The System Controller will delegate functions to the assistant System Controllers when necessary.
- f) However, the overall responsibility resides to the main System Controller.



8. ROLES AND RESPONSIBILITIES

The roles and responsibilities pertaining to the use and management of BAS are as follows:

a) The responsible CFO Must:

- I. Review quarterly reports from the System controller and System Owner
- II. Endorse PPT compliance certificate after checking quarterly reports.
- III. Recommend re-training of System controller and/or Assistant System Controller.
- IV. Initiate internal audit review where necessary.
- V. Initiate Security and Anti-corruption system spot checks

b) The responsible Senior Manager/ System Owner Must:

- I. Ensure that the System Controller and his/ her Assistant are appointed in writing.
- II. Ensure that the System Controller and his/ her assistant are trained.
- III. Ensure that the System Controller and his/ her assistant are vetted.
- IV. Ensure development, implementation and ensure adherence to provincial policies and procedures.
- V. Implement proper processes for internal control and risk management.
- VI. Monitor activities of the System controller through monthly reports.
- VII. Review BAS quarterly reports prepared for the CFO.

c) The responsible System Controller Must:

- I. Ensure maintenance of user IDs for all BAS users.
- II. Ensure transgression to the policy is reported to the Senior Manager for necessary action.
- III. Reset password for users who have been revoked.
- IV. Review all user profiles on quarterly basis.
- V. Provide a report to the Senior Manager for submission to PPT.
- VI. Ensure orientation of new BAS users on the policy and procedures is done.
- VII. Ensure that all BAS users and supervisors are properly trained.
- VIII. Provide access control for users in security profiles and budget profiles.
- IX. Ensure proper processes of resetting users are adhered to.
- X. Ensure his or her password is safeguarded
- XI. Document all relevant maintenance on user/ group profiles.



- XII. Ensure that maintenance of functions assigned to users according to his/her job descriptions.
- XIII. Detect and investigate any inactive users.
- XIV. Maintain departmental SCoA (code structures) and parameters.
- XV. Liaise between source systems (LOGIS and PERSAL) and BAS when implementing interfaces
- XVI. Be aware of and facilitate all BAS releases unless PPT directs otherwise
- XVII. Distribute BAS notices and bring important issues to the attention of management within their respective divisions.
- XVIII. Facilitate the clearing of exceptions.
- XIX. Enforce segregation of duties.
- XX. Investigate any cases of access violations
- XXI. Link printers to BAS for printing reports
- XXII. System Controller must not:
 - Conduct desktop support
 - Administering the network
 - Maintaining the files and address server problems
 - Installing BAS
 - Executing functional transactions

d) The responsible Assistant System Controller must:

- I. Assist the System Controller with all the duties outlined on 8c.
- II. Follow due processes when resetting the System Controller user ID.

e) Responsibilities of DGITO Must only be:

- III. To install BAS upon receipt of a written request from BAS System Controller
- IV. To update Codes Tables when required by National Treasury
- V. Administering the network
- VI. Maintaining the files and address server problems
- VII. Setup printers for BAS linkage
- VIII. Inform BAS System Controller when CoGTA increases IP address range



f) Responsibilities of BAS Capturers Must Only be:

- I. To capture/ maintain transactions on BAS.
- II. To request BAS reports and perform enquires.
- III. Safeguarding his/ her user ID and password.

g) Responsibilities of BAS Supervisors/ Authorisers Must Only be:

- I. To verify and authorise/ reject transactions captured on BAS.
- II. To request BAS reports and perform enquiries.
- III. Safeguarding his/ her user ID and password.

9. USER ACCOUNT BAS MANAGEMENT

a) CREATING A NEW SYSTEM CONTROLLER USER ID

- I. The new System Controller User ID can only be created by NT upon receiving a written request from the departmental CFO.

b) PROVISION OF ACCESS TO THE ASSISTANT SYSTEM CONTROLLER

- I. The department shall nominate/ appoint an Assistant System Controller who takes over the System Controller's responsibility in the event that the System Controller is absent from the office.
- II. Assistant System Controller should be registered with NT and PPT by following proper procedure.

c) CREATION OF NEW USERS/ GROUP PROFILE

- I. New Users will only be granted access to the system upon completion and submission of a duly authorised application form.
- II. For users employed outside of Finance and Supply Chain a signed memorandum from the user's supervisor detailing why access must be granted and how this will not affect the segregation of duties.
- III. All details and access needs must be clearly stated on the application form to allow the user to be granted the correct profile.

d) AMENDING USERS/ GROUP PROFILE

- I. The System Controller should only amend a user's profile upon receiving a Director approved request from the user.

e) RESETTING USER PASSWORDS

- I. The requests for the password reset should be made in writing.
- II. Proper procedure regarding the resetting must be followed by filling and submitting an approved reset form to the System Controller.

f) DEACTIVATING/ TERMINATING USER PROFILES

- I. Any BAS System Controller who does not adhere to this policy when using BAS or who misuses the system should be immediately deactivated from the system by National Treasury.
- II. The deactivation can be initiated by either the System Owner, CFO, Provincial Treasury or National Treasury.
- III. The Stakeholder that initiates the deactivation has the responsibility to inform other Stakeholders listed on f (ii) above.
- IV. The deactivation is done through logging a call with Logik contact centre at NT requesting the immediate deactivation of the defaulting System Controller from the BAS system, until the investigation into the matter has been finalised.
- V. The Logik contact centre at NT should only reactivate the System Controller after investigation by the relevant department, which clears such a user of any wrong doing, or as directed by departmental CFO or the AO
- VI. The access rights of users who have left the department or have moved to another section should immediately be removed or at the latest 7 days after the vacation of the office.
- VII. Users who do not adhere to the policy or procedure will be de-activated whilst investigations are proceeding.
- VIII. A full report of such incidences should be reported to the PPT.

10.ACCESS VIOLATIONS

- a) System Controller and all BAS Users must guard against access violation on their User IDs
- b) Cases of access violation will be investigated and those found to have violated access will be deactivated from the system and disciplinary action will be instituted against them.

11.CREATION/AMENDMENT OF CODE STRUCTURE

- a) System Controller must only create or amend the code structure upon receipt of a written request from the department, PPT or NT.

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

- a) System Controller must orientate all new users on BAS login procedure immediately after creating such users.
- b) All new users must attend training with PPT within three months of assuming their positions.



14. BAS SECURITY

a) UNATTENDED USER EQUIPMENT

- I. It is the responsibility of each user to safeguard the system and system resources against any unauthorised access.
- II. Users must log off from the system when they are done with the session they were working on before leaving their workstations.

b) SAFEGUARDING OF PASSWORD

- I. User Ids and passwords are the property of the department and users must keep them confidential at all times.
- II. Should the confidentiality of a password be compromised the user must immediately request a password reset from the System Controller.

15. IMPLEMENTATION

- a) This policy shall be implemented on the date of approval by the Member of the Executive Council (MEC).

16. NON-COMPLIANCE

- a) All BAS Users must comply with this policy and each User is responsible for reporting non-compliance.
- b) Non-compliance to this policy will be dealt with in accordance with the public service disciplinary code of conduct.
- c) However consequences may include withdrawal of user accounts, suspension from work, dismissal from public service, or imprisonment depending on the severity of the non-compliance.
- d) System Controller must report all non-compliance matters to the System Owner.

17. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY

- a) The Budget Planning and Management directorate will monitor the implementation of this policy and will report to the departmental CFO on both compliance and non-compliance issues.

18. COMMUNICATION / EDUCATION OF THE POLICY

- a) The BAS Policy will be communicated throughout the department to all BAS users through workshops and other communication channels.

19. DISPUTE RESOLUTION MECHANISM

- a) In the event of disputes arising out of this policy, such disputes will be dealt with in terms of the grievance procedure and labour legislation applicable in the Public Service.



20. APPROVAL OF THE POLICY

- a) The policy shall be recommended by the AO and approved by Member of Executive Council (MEC) as per the updated departmental delegations.

21. REVIEW OF THE POLICY

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

VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (the date the policy takes effect)	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.
2014		MEC	
2015			
2016		MEC	Section 8a Section 8b (iii, vi, vii) Section 8c (xx) Section 9f (vi) Section 10 Section 16a, d
2017			Section 8a (v) Section 8c (xxi) Section 8d Section 8e (i to vi) Section 8f (iii) Section 8g (iii)