Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

Supply Chain Management
Tyamzashe Building | Civic Square | Bisho | 5605
P/Bag X0035 | Civic Square | Bisho | 5605
Tel: +27 (0)40 940 7028 / 7029 | Fax: +27 (0)40 635 1515

SUPPLY CHAIN MANAGEMENT UNIT

LOGIS POLICY

DEPARTMENTAL CONTACT DETAILS	
Physical Address	Department of Cooperative Governance and Traditional Affairs Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Cooperative Governance and Traditional Affairs Private Bag X0035 Bhisho 5605
Document No.	01
Document Name	LOGIS Policy
Contact Person	Mr S. Mathumbu
Designation	Director: Supply Chain Management
Directorate	Supply Chain Management
Telephone No.	040 – 940 7008
Cell Phone Number	071 604 3366
E-mail Address	SCM@eccogta.gov.za
Date of approval	
Date last amended	14 December 2018
Date for next review	As and when the need arises
Related Policies	Supply Chain Management Policy

Table of Contents

SIGN OFF

I. HEAD OF DEPARTMENT

The LOGIS Policy has been recommended by Mr V. Mlokothi, in his capacity as the Accounting Officer for the Eastern Cape Department of Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the content of this policy.

Based on the Public Service Supply Chain Management Legislation, development of this LOGIS Policy will ensure that the department is able to exercise its powers in compliance with the law and guide decision-making in the organization.

Signed:	
Designation:	Acting Head of Department for the Eastern Cape Department of Cooperative Governance and Traditional Affairs: Mr V. Mlokothi
Date:	24/03/2025

II. EXECUTIVE AUTHORITY

The Department of Cooperative Governance and Traditional Affairs has unprecedented opportunity to improve the livelihoods 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 the challenges of its people.

I therefore trust that guidance from the LOGIS Policy will contribute to the efficiency of the department.

Signed:	
Designation:	Honourable MEC for Department of Cooperative Governance and Traditional Affairs: Mr Z. Williams
Date:	26/03/2025.

1. INTRODUCTION

The Logistical Information System (LOGIS) is one of the three Transversal Financial Information Systems utilized by the South African Government. LOGIS is utilized for Supply Chain Management and consists of three modules, namely, Procurement Integration, Inventory Management and Asset Management. The normal day-to-day operations of LOGIS are the responsibility of the department executed by a designated departmental system controller. Provincial Treasury is responsible for the rendering of LOGIS transversal support services (training, user support, monitoring and implementation) to all departments within the Provincial Government of the Eastern Cape.

2. PURPOSE OF THE POLICY

Vital to the integrity of LOGIS is the implementation, maintenance and management of proper system controls. Without effective systems controls, the integrity of the LOGIS environment may be compromised due to override, circumvention, or modification of associated controls. This LOGIS policy has therefore been developed to ensure that there are adequate internal controls to safeguard access to and ensure responsible use of the LOGIS by all users.

3. BACKGROUND

Provincial Treasury has issued an Instruction Note on Logis Information System (LOGIS) and User Account Management (Provincial Treasury Instruction Note No. 4 of 2024/25) governing the use of LOGIS in all Eastern Cape Government Departments. This policy is aligned with the international best practice as well as the Office of the Auditor General Best Practice Guide for User Account Management of 2010.

4. SCOPE

This policy is applicable to all users of LOGIS and delegated employees who oversee management of the system in the department. These include, but not limited to:

- Accounting Officer;
- Chief Financial Officer;
- Head of Supply Chain Management Unit;
- Programme Managers;
- System Controller;
- Users / Capturers;

- Supervisors / Authorisers;
- Internal Audit; and
- Contract Workers/ Interns/ Learners

5. DEFINITION OF TERMS

Meanings and definitions of terms used in this document are provided below:

"AGSA": Auditor General South Africa;

"BAS": Basic Accounting System;

"FIS": Financial Information Systems;

"CFO": Chief Financial Officer;

"LOGIS": Logistical Information System;

"RACF": Resource Access Control Facility;

"User ID": Unique code allocated to a user in order to access the system.

"User Profiles": The level of access allocated to a user.

"System Controller": 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;

"**System Owners** (Head of SCM/delegated employee"): Director: SCM Unit who is responsible to monitor the head office Systems Controller monthly;

"User": An employee/person who has a user id to access LOGIS for capturing, authorizing transactions updating or amending system data and extracting management information from LOGIS;

"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 its own needs.

"POPI Act": Protection of Personal Information Act (POPI ACT No 4 of 2013)

"PERSAL": Personnel and Salary System

"LOGIS releases": Enhancements on LOGIS

"DGITO": Departmental Government Information Technology Officer;

"SITA": State Information Technology Agency;

"RO033": Security Profile Report

"RR121": Security user profile report;

"RR122": Security user profile history report;

"RR123": RACF id report;

"RR124": RACF Id history report;

"RR125": Allocated functions for active user's report;

"RR127": History of allocated functions;

"ENAD": Audit Trail Enquiry selection;

"IDCI": RACF ID maintenance selection

6. LEGAL FRAMEWORK

6.1 Section 18 (1) (c) of the PFMA requires Provincial Treasury to promote and enforce transparency and effective management in respect of revenue, expenditure, assets and liabilities of provincial departments.

6.2 Section 18 (2) (b) of the PFMA requires Provincial Treasury to enforce the Act and any prescribed national and provincial norms and standards, including any prescribed standards of Generally Recognized Accounting Practice (GRAP) and uniform classifications systems, in provincial departments.

6.3 Section 38 (1) (a) of the PFMA requires the accounting officer to ensure that the department, has and maintains:

6.3.1. Effective, efficient and transparent systems of financial and risk management and internal control.

6.3.2. An appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective.

6.4 Section 40 (1) (a) requires the accounting officer for a department to keep full and proper records of the financial affairs of the department in accordance with prescribed norms and standards.

7. OVERVIEW OF LOGIS

7.1 LOGIS is implemented in the department according to the level of transactional responsibility. Therefore, should a department have districts or institutions that run their own budgets on BAS they will require a separate LOGIS Store per regional office.

7.2 LOGIS consists of three modules – Procurement, Assets and Inventories Modules.

The following user types exist for LOGIS:

Table 1 – LOGIS User Types and Functions

User Type	***Function***
User Type 1 System Administrator (Based at National Treasury)	• Responsible for creating other User Type 1 IDs and User Type 6 profile. • Responsible for creating/managing User Type 2 profiles.
User Type 2 Departmental System Controller (Based at Provincial Treasury)	• Full Enquiry & Report Functionality access. • Responsible for creating/maintaining and monitoring User Type 7 profiles (Departmental System Controller). • Access to all the stores in Province.
User Type 3 Store Specific System Controller (Sub – System Controller)	• Responsible for creating/maintaining and monitoring User Type 4 & 5. • Access to all LOGIS Functionality. • Only has access to specific store in the Department they are linked to.
User Type 4 Capture/ Authorize Employee	• Access to LOGIS Functionality as specified on SASP. • Only has access to specific store in the Department they are linked to.
User Type 5 Cost Centre Employee	• Access to LOGIS Functionality as specified on SASP. • Only has access to specific store in the Department they are linked to.
User Type 6 Special User IDs (Based at National Treasury)	• Must be able to create, modify or delete Central Items, Suppliers. • Contracts and Management Information Item numbers - these items are then accessible to all Departments. • May be able to perform some System administration (e.g. Utilities).
User Type 7 System Controller	• Access to multiple stores. • Access to administrative enquiries and reports. • Creation and maintenance of User profiles in the stores they have access to. • Created, monitored and maintained by User Type 2.
User Type 8 Departmental Asset/ Inventory Manager	• Access to transaction over multiple stores in Department. • Grant of access to stores & functions must be maintained by User type 7 with SAPS or User Type 2.

To successfully maintain LOGIS in a department, the System Controller (User Type 7) must be appointed at Head Office in the department. However, each LOGIS Store within a department requires its own LOGIS Store Specific System Controller (Sub-System Controller User Type 3) who must be correctly appointed and trained.

8. ROLES AND RESPONSIBILITIES

The roles and responsibilities pertaining to the utilisation and management of LOGIS are as follows:

8.1 CHIEF FINANCIAL OFFICER

8.1.1 The Chief Financial Officer or a delegated employee in the department is responsible for the appointment of a System Controller, Store Specific System Controller (Sub-System Controller) for LOGIS and to also ensure that prescribed policies and procedures are in place and adhered to.

8.1.2 The duties of the departmental CFO regarding the System Controller(s) include:

8.1.2.1 Familiarizing himself/ herself with the duties of the LOGIS System Controller.

8.1.2.2 Regular monitoring of the duties and activities of the System Controller(s) to ensure that it is executed in accordance with the prescribed procedures and that the control measures are maintained.

8.2 DEPARTMENTAL SYSTEMS OWNER

The Departmental Systems Owner is an employee responsible to monitor the activities of the System Controller user account management activities. Furthermore, the Departmental Systems Owner facilitates the appointment of a relief System Controller in absence of a System Controller.

8.3 SYSTEM CONTROLLER

8.3.1 The System Controller is an employee who resides at the department using LOGIS. All System Controllers are ultimately responsible to the departmental CFO for their actions. He/she must ensure smooth and appropriate operation of LOGIS in the department.

8.3.2 The primary tasks of the System Controller are:

8.3.2.1 Maintenance of user IDs for employees listed below is subject to the completion and approval of a **user application form**, and a formal **written undertaking** by the user to safeguard their password:

i. Sub- System Controllers.

ii. A person employed within the Public Service is required to work on LOGIS performing functions relevant to their duties;

iii. A contract worker or intern employed by a department who requires access.

8.3.2.2 Deny, terminate or temporarily withdraw a user's access to LOGIS if:

i. There is suspected misuse of his/her user ID;

ii. There is suspected fraudulent activity;

iii. A user ID is not utilized for a period of 30 days and;

iv. Upon resignation of the relevant user (termination of employment)

8.3.2.3 Review all user profiles on a monthly basis. System Controllers must provide a quarterly compliance certificate on user account management with supporting documents (quarterly report to the CFO and user account management questionnaire) to Provincial Treasury Financial Information Systems, indicating that all active users on LOGIS are a true reflection of the department's employees, who are permitted access, in accordance with their profiles.

8.3.2.4 The LOGIS System Controller is responsible for the on the job training of new LOGIS users.

8.3.2.5 Ensure that all LOGIS users and supervisors in the department are properly trained. This includes continuous training when enhancements are effected and the submission of formal training requests to Provincial Treasury.

8.3.2.6 Responsible for the maintenance of functions assigned to users according to his/her job descriptions as per formally approved instruction.

8.3.2.7 Ensure that the disaster recovery test is performed periodically as per SITA Circulars.

8.3.2.8 Detect and investigate any dormant users.

8.3.2.9 Distribute LOGIS notices and bring important issues to the attention of management within their respective departments.

8.3.2.10 Facilitate the clearing of interface exceptions.

8.3.2.11 Grant users with access to functions relevant to their duties.

8.3.2.12 Jointly responsible for compiling and maintaining a departmental procedure manual.

8.3.2.13 Monitoring effective use of LOGIS.

8.3.2.14 Liaise between departmental users and Provincial Treasury.

8.3.2.15 Provide guidance to all users within the department.

8.3.2.16 Assist with the administration of LOGIS implementation.

8.3.2.17 Enforce segregation of duties within the department.

8.3.2.18 The LOGIS System Controller also has the ultimate responsibility to ensure that his own user ID and password is safeguarded against unauthorized access.

8.3.3 Please note that the System Controller's responsibilities do NOT include:

8.3.3.1 Administering the Network.

8.3.3.2 Maintaining the file and address servers.

8.3.3.3 Installing LOGIS.

8.4 LOGIS USER/ CAPTURER

8.4.1 To capture/ authorize transactions on LOGIS.

8.4.2 To request LOGIS reports and perform enquiries.

8.4.3 A user must log off each time he/she is not utilizing LOGIS to prevent misuse of his/her ID's.

8.4.4 At all times a "Complex password" must be utilized.

8.4.5 Change passwords frequently at least every (30) working days.

8.4.6 ID's and passwords are solely for the relevant user's access to LOGIS and must be used in a responsible manner and never shared with any other person under any circumstances. Should it become known that users are sharing their password/s, immediate disciplinary action must be instituted against the user/s. A full report of such action must be provided to the Provincial Treasury, via the Departmental System Controller/ functional managers.

8.5 LOGIS SUPERVISOR/ AUTHORIZER

8.5.1 To verify and authorize/reject transactions captured on LOGIS.

8.5.2 To request LOGIS reports and perform enquiries.

9. NEW LOGIS USERS

9.1 New users will only be granted access to the system upon completion and submission of a duly authorized application form. It is important to note that the application must reflect all relevant information to allow the new user to be allocated with the correct profile on the system. When necessary, a dual user id, approved by the CFO only, may be allocated to a user due to segregation of duty. The onus resides with the department and sound measures must be put in place to avoid misuse of the dual user id.

9.2 New and current users shall be trained according to the Transversal Systems Training Procedure Manual (BAS, LOGIS and PERSAL).

10. MANAGEMENT REPORTING

The LOGIS System Controller shall report every quarter in a prescribed format to the CFO on the status of all active LOGIS users and compliance to the instruction note.

11. USER ACCOUNT MANAGEMENT: ROLE OF CLIENT DEPARTMENT

11.1 The user account management processes for LOGIS are detailed below. These procedures cover the roles and responsibilities of the following:

11.1.1 System Controller,

11.1.2 Systems Owner, and

11.1.3 The Chief Financial Officer of the Department.

12. FUNCTIONS OF THE SYSTEM CONTROLLER

12.1 The System Controller is the responsible employee for compliance with LOGIS related matters e.g., correct configuration of the system, user account management, liaise with the users in the Department, Provincial Treasury and National Treasury. A System Controller is ideally an advanced LOGIS user and has successfully passed the LOGIS System Controller Course.

12.2 **The System Controller has the following responsibilities:**

12.2.1 Keep a list of all dual ID's for audit purposes.

12.2.2 Maintain a list for all profiles created and terminated.

12.3 **Draft a monthly report to the System Owner on following activities:**

12.3.1 New user registration.

12.3.2 User profile amendments.

12.3.3 User login violations.

12.3.4 User deregistration / terminations.

12.3.5 Password Management.

12.4 Keep a monthly file on all newly created and terminated users. The file must consist of an index page displaying the reference number and include description to use as input to the system. The reference number must have the abbreviation of the department name. The file must consist of duly completed and authorized new user access forms (system input documents) per new user and reconciled to the system generated report on new users:

12.5 NEW USER REGISTRATION

12.5.1 New users will only be granted access to the system upon completion and submission of a duly authorized application form. Newly created users must go for formal LOGIS training within three months. In the event where formal training is not possible at that stage the department undertakes to provide system orientation and person to person training to the user until such time that that formal training is undertaken. The System Controller must ensure that training nominations including new users is sent to Provincial Treasury.

12.5.2 The system input document to create a user on the system must contain at least the following headings and thereafter it must be reconciled with the system generated report (RO033):

i. Name of department / store number.
ii. Name & surname of user.
iii. South African ID number of the user.
iv. PERSAL number of users.
v. Level of access indicating segregation of duties.
vi. Contact details of the user.
vii. Signature of the user.
viii. Signed recommendation of the supervisor & signed approval by the System Controller.

12.5.3 The input document must contain a declaration of secrecy whereby the user attests to being fully responsible for the allocated functions. A User will adhere to the relevant policies and procedures and will formally report any potential fraud / identity theft / misconduct on the system as and when such instances are identified.

12.5.4 The input document together with the list of selections must be attached to a memorandum from the supervisor requesting system access for the user. The memorandum must clearly define the areas of access required and must indicate how these areas of access will not compromise segregation of duties as per attached annexure A.

12.5.5 Additional to the form, copy of user's South African ID / PERSAL Print Out 4.3.1

12.5.6 Ensure that all LOGIS users in their department are properly trained within 3 months.

12.6 USER PROFILE AMENDMENTS

12.6.1 The system input document to modify a user on the system must contain at least the following headings and thereafter it must be reconciled with the system generated report (RO033):

12.6.2 Keep a monthly file on all profile amendments. The file must consist of an index page displaying the reference number and include description to use as input to the system. The reference number must have the abbreviation of the department name.

12.6.3 In the events of temporally amendments on the role of the user due to departmental changes a period must be specified for the profile amendments on the memo from the supervisor.

12.7 USER LOGIN VIOLATIONS

12.7.1 Receive RACF Report (User Activity Download Report) of all Login violations.

12.7.2 System Controller must identify and investigate three (03) or more repeated Login violations per user and report in writing on the root cause of each situation in the live production environment. Maintain evidence of remedial action taken e.g., user re-training etc.

12.7.3 System Controller to verify in the attendance register or any means that the user was on duty on date of violation. A copy of attendance register must be attached as evidence.

12.7.4 Report must clearly establish whether a trend exists and identify the root cause and show intervention taken.

12.7.5 In exceptional cases where there is no submission of the authentication form, the System Controller can soft lock or put on leave a user with reason code 01. Once the form has been submitted the System Controller will restore the profile of the user, with the necessary input documentation (i.e., Request Memo, Copy of ID, Log 21 form, RR121 Report).

12.8 USER DE-REGISTRATION

12.8.1 System Controller request System report (RR121) on user profiles for all users (which outlines all active and inactive users) to identify the following:

12.8.2 Identify all dormant users that did not access the system within 30 days.

12.8.3 Terminate all dormant users.

12.8.4 Prior to terminating the dormant user from the system, the user must be informed in writing via the supervisor stating the reasons.

12.8.5 Users that do not operate actively in all modules must log onto the system at least once a month on all access levels.

12.8.6 In the event where a user is no longer in the employ of the department and the System Controller was not informed prior to the departure, the LOGIS Office must complete the Input Document to deregister the user.

12.8.7 On exception where there is no feedback from supervisors and dormant users cannot be reached, System Controller can complete an input document with a list of dormant users and attach report RR121 for deregistration on the system.

12.9 MONTHLY SERVICE TERMINATION RECORD FROM PERSAL

12.9.1 Obtain monthly Service Termination record from PERSAL Controller.

12.9.2 Obtain monthly Terminations Route List from the Human Resource department.

12.9.3 Obtain system generated report on all users and compare all the active users on the system to the PERSAL Termination Report.

12.9.4 Terminate all users on the system that appear on the PERSAL Service Termination Report.

12.9.5 Evidence of Termination – duly authorized deregistration forms must be submitted to the System Controller as an input document to deregister a user on the system

12.10 PASSWORD MANAGEMENT

12.10.1 Users reset their own password on Portal according to LOGIS notice 4 of 2014.

12.10.2 In the event where a user is unable to reset his/her password on LOGIS Portal for self-reset the System Controller will reset users on the mainframe and the following headings must appear on the application form (Log 25).

12.10.3 Name & surname of the user.

12.10.4 Department / store number.

12.10.5 User ID, contact detail of the user.

12.10.6 Signature of user, date.

12.10.7 Name and surname of System Controller, date reset.

12.10.8 The password reset application form must be completed and must be signed off by both the user and the System Controller.

12.10.9 The input document must contain a declaration in accordance with the Protection of Personal Information Act (POPI ACT No 4 of 2013).

12.10.10 All system exceptions related to user account Management to be formally approved by the CFO or his / her Delegatee in writing.

12.11 QUARTERLY REVIEW OF ALL USERS ON THE SYSTEM

12.11.1 Systems Controller must send user review forms to all users with the following headings:

i. Name and surname of the user.

ii. Department/store number, user id.

iii. User type/access level.

iv. System responsibility.

v. SA ID number.

vi. Date, signature of user.

vii. Signature of System Controller.

12.11.2 Form to be countersigned by users' supervisor.

12.11.3 Form to cover access levels to confirm functional areas to perform duties i.e., does the user still require access to the payment functionality on the system or has his/her job function changed.

12.11.4 Compare the authentication form with the profile of the user.

12.11.5 Effect the changes immediately upon receipt of the review forms.

12.11.6 Submit monthly reports on user account management to system owner for all months in the quarter.

12.11.7 System Controller must prepare and submit quarterly report on User Account Management for the department for signature of the CFO.

12.11.8 Submit the Quarterly Compliance Certificate to Provincial Treasury within 7 working days after end of the quarter.

12.11.9 In exceptional cases where there is no submission of the authentication form, the System Controller can soft lock or put on leave a user with reason code 01. Once the form has been submitted the System Controller will restore the profile of the user, with the necessary input documentation (i.e., Request Memo, Copy of ID, Log 21 form, RR121 Report).

12.12 FUNCTIONS OF THE DEPARTMENTAL SYSTEMS OWNER

12.12.1 Receive, review, approve monthly report and monitor the activities of the System Controller with regards to:

i. User profile amendments.

ii. User login violations.

iii. User deregistration.

iv. Password management.

v. New user registration.

12.12.2 Review quarterly report from the System Controller to the CFO that provides assurance that all requisite user account management activities have been performed and endorse it accordingly.

12.13 FUNCTIONS OF THE CHIEF FINANCIAL OFFICER

The Chief Financial Officer has the following responsibilities with regards to User Account Management:

12.13.1 Review quarterly report from System Controller and System Owner.

12.13.2 Initiate clear action and consequence management where necessary.

12.13.3 Recommend for re-training of System Controller / System Owner.

12.13.4 Initiate an internal audit review where there is consistent failure by the System Controller and System Owner to adhere to the User Account Management Policies and Procedures.

12.13.5 Sign the Provincial Treasury User Account Management Compliance Certificate that is submitted to the Provincial Treasury by the System Controller.

13. GENERAL REQUIREMENTS

LOGIS User who does not adhere to this LOGIS Policy or who misuses LOGIS should immediately be deactivated from LOGIS by the System Controller, until the departmental investigation into the matter has been finalized. A System Controller should only reactivate the user after investigation by the relevant department, which cleared such user of any wrongdoing, or as directed by the CFO or HOD.

LOGIS System Controllers who misuses their administrative rights as a System Controller should be immediately deactivated from LOGIS upon receiving a written instruction from the CFO at the department to the user type 2 at Provincial Treasury to proceed with the action to deactivate the System Controller.

14. NON-COMPLIANCE

Non-compliance to this Policy and its provisions may constitute financial misconduct and any employee found to be transgressing this policy will be subjected to disciplinary enquiry in terms of the Public Service Act, 1999 (Proclamation 103 of 1994) and other relevant legislation.

15. POLICY REVIEW

This LOGIS Policy shall be reviewed with the issuing of any new instruction note to ensure that it is effective and relevant.