PROCEDURE MANUAL FOR TRANSVERSAL SYSTEMS (LOGIS AND BAS)

FILE NAME	PROCEDURE MANUAL FOR TRANSVERSAL SYSTEMS (LOGIS AND BAS)
ORIGINAL AUTHOR	DEPARTMENT OF CULTURE, SPORT AND RECERATION
REVIEW DATE	1 APRIL 2019

TABLE OF CONTENTS

TABLE OF CONTENT.....1

1. PURPOSE OF THE PROCEDURE MANUAL.....2
2. REGULATORY FRAMEWORK.....2
3. DEFINITIONS.....3-4
4. SCOPE OF APPLICATION.....4
5. PRINCIPLES.....5
6. USER ACCOUNT MANAGEMENT PROCESSES.....6-7
7. ROLES AND RESPONSIBILITIES.....8-10
8. RESPONSIBILITY GRID.....11-12
9. DECENTRALIZED VS CENTRALIZED DEPARTMENTS.....12
10. PASSWORD CONTROLS.....13
11. REVIEW OF THE PROCEDURE MANUAL.....13
12. CONTRAVENTION.....13
13. ANNEXURES ... .14
    - 13.1. DUTIES AND RESPONSIBILITIES OF PROVINCIAL SYSCON
    - 13.2. DUTIES AND RESPONSIBILITIES OF DEPARTMENTAL SYSCON
    - 13.3. DUTIES AND RESPONSIBILITIES OF THE SYSTEM ADMINISTRATOR
    - 13.4. USER REGISTRATION/AMENDMENT FORM
    - 13.5. REGISTRATION OF SYSTEM ADMINISTRATOR FORM
    - 13.6. RESET FORM
    - 13.7. TERMINATION FORM
    - 13.8. HAND OVER FORM
    - 13.9. REVIEWAL OF USERS ACTIVITIES TEMPLATE
    - 13.10. REVIEWAL OF SYSCON ACTIVITIES TEMPLATE

1 Purpose of Procedure Manual

The purpose of this Procedure Manual is to provide documented guidelines required for the management of security profiles in Basic Accounting Systems (BAS) and Logistical Information Systems (Logis) by all Mpumalanga Provincial Government. This Procedure Manual will guide all users who use Basic Accounting System and Logistical Information System.

2 Regulatory framework

2.1. Regulations

Provincial Departments operations are governed by an array of different acts and this manual should be understood within that context.
The following Acts and prescripts are central in defining departmental boundaries and areas of influence:

- Public Finance Management Act, 1999 (Act 1 of 1999).
- National Treasury Regulations.
- National Treasury guidelines and prescripts.

2.2. Guidelines

Good Practice Guide – User Account Management (Auditor General – South Africa)

3 Definitions and Acronyms

In this policy, unless the context otherwise indicates:-

"Accounting officer" means the Head of a Department of Human Settlements appointed in terms of Section 36 of the Act

"Act" means Public Finance Management Act, 1999 (Act No. 1, 1999)

"Group Special Privileges" Persons to whom the RACF has been allocated for the Maintenance of Persal and Logis mainframe IDs
"Province" means Mpumalanga Provincial Government

"Provincial Treasury" means the Provincial Treasury support group

"Revoked," means accounts being inactive due to Logon violations

"System" means the Basic Accounting System

"Decentralized Department" User access rights will be managed by the Department

"Centralized Department" User access rights will be managed by Mpumalanga Provincial Treasury (MPT)

"Provincial System Controllers" means persons allocated with super-users accounts and functions on the system in order to control normal users accounts rights and that person is based at Mpumalanga Provincial Treasury.

"Departmental System Controllers" means persons allocated with super-users accounts and functions on the system in order to control normal users accounts rights and that person is based at the Department whose access rights are decentralized.

"Security profiles" means user accounts allocation on the systems such as IDs, Passwords and functions

"Terminations" means removal of active profiles from the system

"User" means an individual authorized to have access rights on the system in the department to perform functions requiring usage of the system for job performance.

"Workflows" means functions and profiles linked to individual and groups

"BAS" Basic Accounting System

"Logis" Logistical Information System

"Syscon" System Controller

"RACF" Resources Allocation Control Facility

"BAS Administrator" A person nominated by the Department to submit necessary documentations to the system controller at the Provincial Treasury for user account management for BAS and do administrative task on the system. (For Centralized Departments only)

"Logis Representative" A person nominated by the Department to submit necessary documentations to the system controller at the Provincial Treasury for user account management for Logis.

4 Scope of application

Users designated by a department to use the system

Super-users or System Controllers

Senior Managers and Managers

BAS and Logis Representative

BAS Administrators (For only centralized Departments)

5 Principles

5.1. The management of security profiles must be in accordance with the Standards for Information Systems Auditing and Control Association (ISACA).

5.2. The effectiveness of the security profiles management procedures of the Province should conform to the internationally accepted Control Objectives for Information and Related Technology framework and industry best practices.

5.3. The focus areas of the Procedure manual must include but are not limited to user account management processes, which are:

- Registration of new users
- Resetting users passwords
- Amendment of users access rights
- Terminating users access rights
- Hand over process

6 Security Maintenance and Review Process Flow

The security profile maintenance must be a guideline between departmental management, Departmental Representatives, System controllers in Provincial Treasury in order to minimize and control risks emanating from fraudulent and corrupt usage of the transversal systems in the Province.

7 User Account Management Processes

Registration of new users

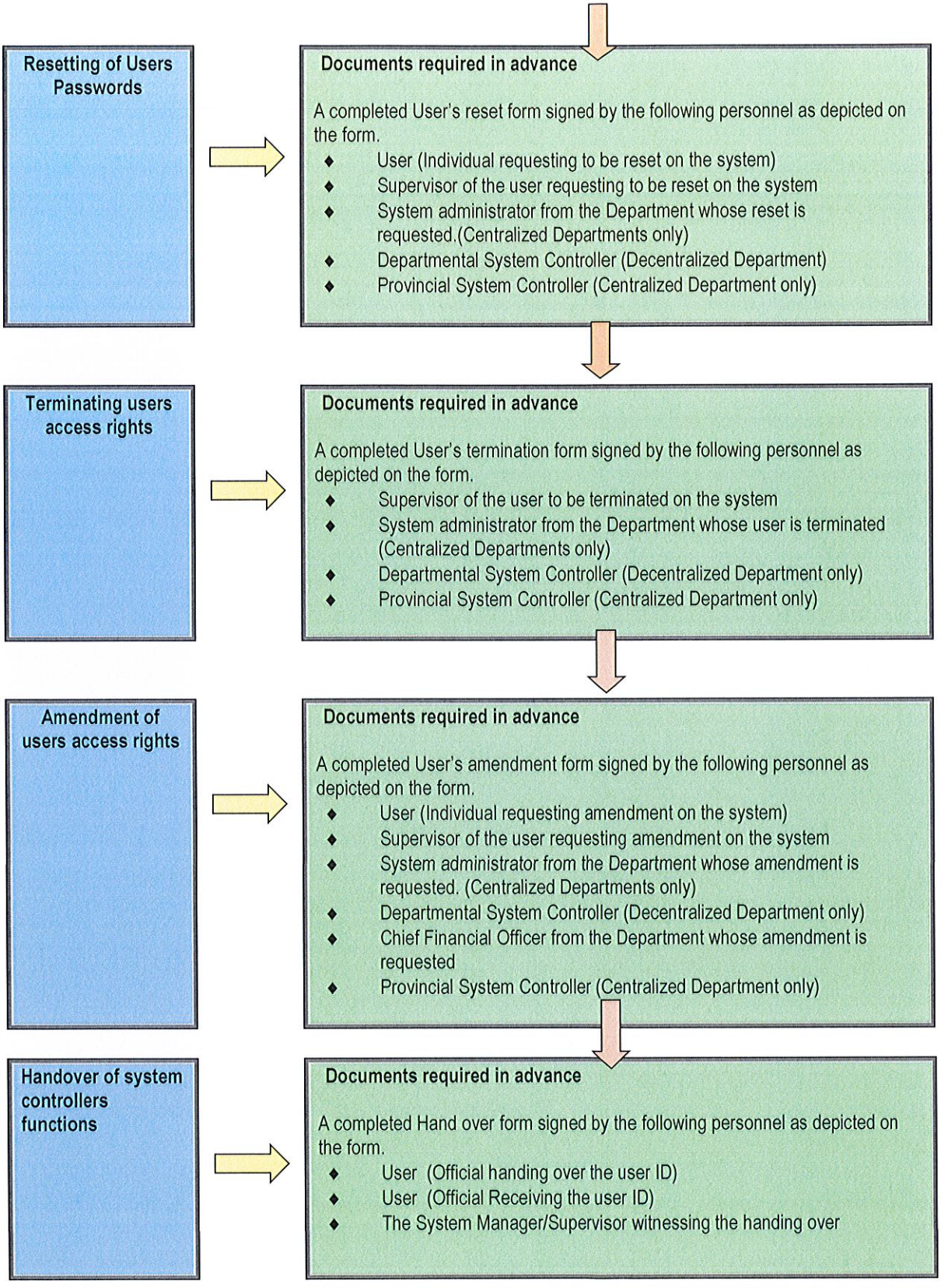
Documents required in advance

1.For the users to be reset by the system controller
A completed User's registration form signed by the following personnel as depicted on the form.

- User (Individual requesting access on the system)
- Supervisor of the user requesting access on the system
- System administrator from the Department whose access right is requested(Centralized Departments only)
- Departmental System Controller (Decentralized Department only)
- Chief Financial Officer from the Department whose access rights is requested
- Provincial System Controller (Centralized Department only)

2.For the users who reset themselves

- No documentations required to be kept by either the user or the syscon.


Resetting of Users Passwords
Documents required in advance
A completed User's reset form signed by the following personnel as depicted on the form.
User (Individual requesting to be reset on the system)
Supervisor of the user requesting to be reset on the system
System administrator from the Department whose reset is requested.(Centralized Departments only)
Departmental System Controller (Decentralized Department)
Provincial System Controller (Centralized Department only)
Terminating users access rights
Documents required in advance
A completed User's termination form signed by the following personnel as depicted on the form.
Supervisor of the user to be terminated on the system
System administrator from the Department whose user is terminated (Centralized Departments only)
Departmental System Controller (Decentralized Department only)
Provincial System Controller (Centralized Department only)
Amendment of users access rights
Documents required in advance
A completed User's amendment form signed by the following personnel as depicted on the form.
User (Individual requesting amendment on the system)
Supervisor of the user requesting amendment on the system
System administrator from the Department whose amendment is requested. (Centralized Departments only)
Departmental System Controller (Decentralized Department only)
Chief Financial Officer from the Department whose amendment is requested
Provincial System Controller (Centralized Department only)
Handover of system controllers functions
Documents required in advance
A completed Hand over form signed by the following personnel as depicted on the form.
User (Official handing over the user ID)
User (Official Receiving the user ID)
The System Manager/Supervisor witnessing the handing over

8 Roles and Responsibilities

7.1. Users

7.1.1. Users must ensure that they do not divulge their security profiles to anybody, including system controllers, fellow users, managers and any persons as this constitute financial misconduct and the users will be liable for any illegal transactions done with their user IDs and / or passwords. The password is like a Bank pin, which the owner must guard against fraud and theft at all, cost.

7.1.2. Users must never under any condition borrow user IDs and passwords to any Persons.

7.1.3. Users must never leave their computers of the financial system open and active as this may be used by other people to perform illegal transactions. A failure to close the system and the resultant usage by other users constitutes negligence and therefore misconduct.

7.1.4. Users must never write their passwords on any visible medium such as a piece of paper attached to the computer or inside the desk. Creating passwords must be simple and easy to remember and retain mentally.

7.1.5. User must inform the syscon/System administrator when the user will not be accessing the system for a specific period.

7.1.6. Users must never use their passwords in the presence of other people watching as this may compromise security of the secrecy of passwords.

7.2. Departmental/Provincial Bas System controllers

7.2.1. Ensure that security profiles are only captured on the system when and if all the documents in point 6 (User account management processes) above are fully completed.

7.2.2. Never perform transactions on the system themselves except those stipulated to be used by the system controllers.

7.2.3. Ensure that proper filling is made for all the security profiles captured on the system.

7.2.4. Ensure that the monthly reset forms send to Provincial Treasury for reset reporting

7.2.5. Monitor and review the activities of the system users on a monthly basis.

7.2.6. Ensure the segregation of duties is properly implemented on the Bas system.

7.2.7. Ensure that the documented procedure manual is made available and understood by the users.

7.2.8. Must report any unusual or suspicious transactions on the system immediately to the Chief financial Officer. Failure to report such abnormal transactions constitute suspected collusion and could be deemed as misconduct or negligence, dereliction of duties, fraud and theft. This may result in charges

7.2.9. Ensure that BAS Password Controls are set as in point 9 (Password controls) below.

7.3. System Managers/Syscon Supervisors

7.3.1. Ensure that the system controller does not have access to production functions, as this constitutes a high risk factor, which must be discouraged at all times.

7.3.2. Monitor the activities of the System Controllers on a monthly basis by ensuring that necessary forms are completed for security profile maintenance and filed accordingly.

7.4. BAS and Logis System Administrator

7.4.1. Ensure that all the user account management forms as depicted in point 6 (User Account Management Processes) above are correctly completed and submitted to Provincial Treasury.

7.4.2. May perform any other function in the Department except user account management.

7.4.3. Ensure that the documented procedure manual is made available and understood by the users.

7.4.4. Must report any unusual or suspicious transactions on the system immediately to the Chief financial Officer. Failure to report such abnormal transactions constitute suspected collusion and could be deemed as misconduct or negligence, dereliction of duties, fraud and theft. This may result in charges and eventual dismissal.

7.4.5. Monitor the activities of the users on a monthly basis.

7.5. Departmental/Provincial Logis System controllers

7.5.1. Prepare and maintain LOGIS system for utilisation: Ensure that BAS is effectively maintained.

7.5.2 Monitor and report on user activities including 3rd party environments: Ensure that the user activity is effectively and regularly monitored, recorded and appropriate actions executed.

7.6. Monitor and facilitate the process of de-committing orders of payments committed without services rendered.

7.7. Support the system provider in user acceptance testing and Disaster Recovery Plan.

7.8. Identify and conduct both informal and formal training of users.

7.9. Provide support in the compilation and maintenance of departmental procedure manuals

7.10. Be the first point of contact between the Department and Provincial Treasury in terms of verifying and submitting necessary documentation for user account management and system related issues

7.11. Make available on regular basis notices, releases, enhancement, progress reports, change control documents and messages to relevant users in the Department.

8. Responsibility Grid

Functions	Interval	Decentralized Department	Centralized Departments	Mpumalanga Provincial Treasury	Reports/ documents
Monitoring of users activities	Monthly	Departmental Systems Controllers	System Administrator	N/A	• Group Profile Report • Login statistics report • Workflow Report • User activity downloads • User profile report
Filling of monitoring of users activities documentary proof	Monthly	Departmental System Controller	System Administrator	N/A	• Completed Users reviewal template.
Security Profile Management (User Registration, resetting, amendment and termination)	Daily	Departmental Syscon	N/A	Provincial Syscon	• Users access rights forms
Filling of Security Profile	Daily	Departmental Syscons	N/A	Provincial Syscons	• Users' access rights forms.

Functions	Interval	Decentralized Department	Centralized Departments	Mpumalanga Provincial Treasury	Reports/ documents
Management (User Registration, resetting, amendment and termination) forms.					
Monitoring of Syscon's activities	Monthly	System Manager or Syscon's Supervisor	N/A	System Manager or Syscon's Supervisor	• Users activity downloads
Filling of monitoring of syscons documentary proof.	Monthly	System Manager or Syscon's Supervisor	N/A	System Manager or Syscon's Supervisor	• Completed Syscon Reviewal template

9. Bas and Logis Decentralised vs Bas and Logis Centralised Departments

With effect from 03 November 2014, Provincial Treasury decentralised the user account management to all the Departments that have an appointed system controller or a fully delegated system controller. The below grid will assist in classifying decentralised and centralised Departments. Centralized Departments user access rights is managed by Mpumalanga Provincial Treasury by the Provincial Syscons where the Department has a system administrator while decentralised Departments have departmental system controllers who manages user access rights for their respective Departments.

Bas & Logis Decentralised Departments	Bas & Logis Centralised Departments
Health	Office Of The Premier
Economic Development	Finance
Safety and Security	Social Development
Education	Sports Logis System Controlle
Sports, Culture and Recreation(Bas Syscon)	
Public Works, Roads and Transport	
Agriculture	
COGTA	
Human Settlements	

10. Password Controls

10.2. The password must be unique to the individual and must not be shared.

10.3. The password length must be at least seven characters.

10.4. The password must be different from at least ten previous used passwords.

10.5. The password must contain characters from uppercase, lowercase, numerals and specials characters in no specific order.

10.6. The password cannot contain spaces or non- anglicized characters.

10.7. The user ID will be revoked after three unsuccessful attempts to sign on.

10.8. Passwords are valid for 30 days.

10.9. A warning will be given before the password expires and the password must be changed by the user.

10.10. Password reset period will be 60 minutes

11. Review of Procedure Manual

This procedure manual will be reviewed annually or whenever the need arises.

12. Contraventions

Any person who contravenes or fails to comply with any provision of this procedure manual may be subjected to disciplinary action through disciplinary processes applicable to the Public Service.

13. Approval

MR. GS. NTOMBELA
HEAD: CULTURE, SPORTS AND RECREARION
DATE: 01/04/2018

ANNEXURE A

1. DUTIES AND RESPONSIBILITIES OF THE PROVINCIAL SYSCON.....16
2. DUTIES AND RESPONSIBILITIES OF THE DEPARTMENTAL SYSCON.....16-17
3. DUTIES AND RESPONSIBILITIES OF THE SYSTEM ADMINISTRATOR.....18
4. DUTIES AND RESPONSIBILITIES OF THE DEPARTMENTAL LOGIS SYSTEM CONTROLLER----------19

5. FORMS ATTACHED
   - 5.1. USER RESET FORM
   - 5.2. USER REGISTRATION/AMENDMENT FORM
   - 5.3. USER TERMINATION FORM
   - 5.4. SYSCON HAND OVER FORM
   - 5.5. BAS SYSTEM ADMINISTRATOR REGISTRATION FORM
   - 5.6. REVIEWAL OF SYSCON'S ACTIVITIES TEMPLATE
   - 5.7. REVIEWAL OF USERS' ACTIVITIES TEMPLATE

1. DUTIES AND RESPONSIBILITIES OF THE PROVINCIAL SYSTEM CONTROLLER

2.

2.1. User account Management: Create and maintained user accounts including user ID, user access, password resets and issuing of functions to the users.

2.2. Workgroup and workflow management: Ensure that Workgroups and workflows are effectively maintained, taking into consideration the; functions, roles, responsibilities and organisational structure and ensuring segregation of duties.

2.3. Provide support in the compilation and maintenance of departmental procedure manuals

2.4. The above task is only done for Centralised Departments

3. DUTIES AND RESPONSIBILITIES OF THE DEPARTMENTAL BAS SYSTEM CONTROLLER

3.1. User account Management: Create and maintained user accounts including user ID, user access, password resets and issuing of functions to the users.

3.2. Workgroup and workflow management: Ensure that Workgroups and workflows are effectively maintained, taking into consideration the; functions, roles, responsibilities and organisational structure and ensuring segregation of duties.

3.3. Provide support in the compilation and maintenance of departmental procedure manuals

3.4. Prepare and maintain BAS system for utilisation: Ensure that BAS is effectively maintained, including; transaction processing rules, item processing rules, item function rules, parameters and linking printers to users, and the facilitation of 3rd party interfaces

3.5. Implement and maintain the departmental chart of accounts: Ensure that the Chart of accounts is effectively maintained and aligned to relevant structures in order to meet the reporting requirements of relevant stakeholders in accordance with relevant legislative requirements.

3.6. Monitor and report on user activities including third party environments: Ensure that the user activity is effectively and regularly monitored, recorded and appropriate actions executed.

3.7. Monitor and facilitate the clearing of interface exceptions, control and suspense accounts.

3.8. Support the system provider in user acceptance testing and Disaster Recovery Plan.

3.9. identify and conduct both informal and formal training of users

3.10. Provide support in the compilation and maintenance of departmental procedure manuals

3.11. Be the first point of contact between the Department and Provincial Treasury in terms of verifying and submitting necessary documentation for user account management and system related issues.

3.12. Make available on regular basis notices, releases, enhancement, progress reports, change control documents and messages to relevant users in the Department.

4. DUTIES AND RESPONSIBILITIES OF THE BAS SYSTEM ADMINISTRATOR

4.1. Prepare and maintain BAS system for utilisation: Ensure that BAS is effectively maintained, including; transaction processing rules, item processing rules, item function rules, parameters and linking printers to users, and the facilitation of 3rd party interfaces

4.2. Implement and maintain the departmental chart of accounts: Ensure that the Chart of accounts is effectively maintained and aligned to relevant structures in order to meet the reporting requirements of relevant stakeholders in accordance with relevant legislative requirements.

4.3. Monitor and report on user activities including third party environments: Ensure that the user activity is effectively and regularly monitored, recorded and appropriate actions executed.

4.4. Monitor and facilitate the clearing of interface exceptions, control and suspense accounts.

4.5. Support the system provider in user acceptance testing and Disaster Recovery Plan.

4.6. Identify and conduct both informal and formal training of users.

4.7. Provide support in the compilation and maintenance of departmental procedure manuals

4.8. Utilise BAS to capture accounting transactions, control the general ledger, closing the month/year, perform financial administration, prepare financial reports and provide any productive function as stipulated by the Department, as the BAS Administrator is not a super user.

4.9. Be the first point of contact between the Department and Provincial Treasury in terms of verifying and submitting necessary documentation for user account management and system related issues.

4.10. Make available on regular basis notices, releases, enhancement, progress reports, change control documents and messages to relevant users in the Department.

5. BAS AND ALOGIS DUTIES AND RESPONSIBILITIES OF THE PROVINCIAL LOGIS SYSTEM CONTROLLER

5.1. User account Management: Create and maintained user accounts including user ID, user access, password resets and issuing of functions to the users.

5.2. Workgroup and workflow management: Ensure that Workgroups and workflows are effectively maintained, taking into consideration the; functions, roles, responsibilities and organisational structure and ensuring segregation of duties.

5.3. Provide support in the compilation and maintenance of departmental procedure manuals.

5.4. The above task is only done for Centralised Departments

6. DUTIES AND RESPONSIBILITIES OF THE DEPARTMENTAL LOGIS SYSTEM CONTROLLER

6.1. Prepare and maintain LOGIS system for utilisation: Ensure that Logis is effectively maintained users, and the facilitation of 3rd party interfaces.

6.2. Monitor and report on user activities including 3rd party environments: Ensure that the user activity is effectively and regularly monitored, recorded and appropriate actions executed.

6.3. Monitor and facilitate the process of de-committing orders of payments committed without services rendered.

6.4. Monitor and facilitate the process of de-committing orders of payments committed without services rendered.

6.5. Support the system provider in user acceptance testing and Disaster Recovery Plan.

6.6. Identify and conduct both informal and formal training of users.

6.7. Provide support in the compilation and maintenance of departmental procedure manuals

6.8. Be the first point of contact between the Department and Provincial Treasury in terms of verifying and submitting necessary documentation for user account management and system related issues.

6.9. Make available on regular basis notices, releases, enhancement, progress reports, change control documents and messages to relevant users in the Department.