Province of the
EASTERN CAPE
DEPARTMENT OF RURAL DEVELOPMENT AND AGRARIAN REFORM

Enquiries:
Chief Director: Supply Chain Management
834 Dukumbana Building
Private Bag X0040 • Bhisho • 5605 • REPUBLIC OF SOUTH AFRICA
Tel. No. (040) 602-5154/5 FAX (040) 602-5128
Email: Sibongile.mzantsi@drdar.gov.za

PROVINCIAL LOGISTICAL INFORMATION SYSTEM (LOGIS) POLICY

Adopted by: Mr B Dayimani
Acting Head of Department
Rural Development and Agrarian Reform

APPROVAL PAGE

APPROVED BY:

MR B DAYIMANI
DATE 02-07-2019
ACTING HEAD OF DEPARTMENT

rural development
& agrarian reform

Department:
Rural Development & Agrarian Reform
PROVINCE OF THE EASTERN CAPE

OFFICE OF THE HOD

Dukumbena Building · Independence Avenue · Private Bag X0040 · BHISHO, 5606 · REPUBLIC OF SOUTH AFRICA.
Tel: +27 (0)40 602 5006/7 · Fax: +27 (0)40 6350604 · E-mail: Zoleka.Makina@drdar.gov.za / Chera-Lee.Oliver@drdar.gov.za
· www.drdar.gov.za

01 July 2019

The Deputy Director General: Rural Development
Mr. B. Dayimani
10th Floor Dukumbana Building
BHISHO
5605

Dear Mr Dayimani,

APPOINTMENT AS ACTING HEAD OF DEPARTMENT

It affords me great pleasure to inform you that you are hereby appointed as Head of Department in terms of Section 37 & 38 of the Public Finance Management Act, Act 1 of 1999 as amended by Act 29 of 1999, Section 32(1) & (2) of the Public Service Act 1994, as amended, and the Executive Authority Delegations to Head of Department for Public Management and Administration 2016, page 8.

Your acting appointment will be for the period 02 to 10 July 2019.

Kindly ensure that all pending matters are attended to.

Kind regards

MS Z. MAKINA
ACTING HEAD OF DEPARTMENT
RURAL DEVELOPMENT & AGRARIAN REFORM

TABLE OF CONTENTS

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 each 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. Further to this, Provincial Treasury is the liaison between the respective provincial departments and National Treasury (the national principle of transversal systems) with regard to all aspects of LOGIS utilisation.

Vital to the integrity of all three Transversal Financial Information Systems is the institution and management of proper systems controls. Without effective systems controls, other controls may be rendered ineffective by override, circumvention or modification.

Previous assessments and reviews have highlighted a lack of effective management of transversal systems at departmental level. This notwithstanding the efforts by Provincial Treasury to utilise training interventions, system circulars, user forums and workshops to emphasise the importance of executing the functions in accordance with the prescribed procedures and processes. Previous Auditor-General reports have highlighted findings that transversal systems are not properly managed and utilised at departmental level due to shortcomings such as the following:

- Departmental policy is not in place to guide and direct access to the systems (who gets access to the systems and under which conditions);
- Lack of documented departmental procedures and defined responsibilities for the management of system users (application form, approval, termination, etc.);
- System users are given access to the systems without receiving any formal training;

- System users are given access to the systems under more than one user identification (undermining segregation of duties);
- Access to the systems are not monitored and evaluated on a regular basis (system users that left the service of departments are still active on the system);
- No procedures are in place to report and follow up on any access and logon violations (possible irregularities/ fraud);
- The actions of Systems Administrators are not monitored;
- The usage of the system is not monitored.

The demarcation of roles and responsibilities pertaining to the management of transversal financial systems are as follows:

ROLE PLAYER	ROLE/ RESPONSIBILITY	
Provincial Treasury	1.1	Implement a generic policy pertaining to access and system security.
	1.2	Standardise system structures throughout departments to facilitate management information and reporting requirements.
	1.3	Limit/ refuse access to new/ current users who have not completed the required formal training in accordance with his/ her profile.
	1.4	Liaison between provincial departmental system controllers and National Treasury
	1.5	Monitor the activities of all provincial departmental systems controllers
	1.6	Render a provincial user support function
	1.7	Implement effective user account management: • Standardise user I.D's to PERSAL number; • Standardise password length; • Standardise password expiry period; • Deactivate dormant users in service as well as users who have left the service; • Catalogue/ request specific reports on a monthly basis that requires on-going attention by departments/ institutions (open commitments).
Departmental System Controller	2.1	Orientation of departmental system users.
	2.2	Identification of training needs and provide person-to-person training.
	2.3	Evaluate and recommend system enhancements.
	2.4	Distribute system notices/ circulars and emphasise issues that require attention.
	2.5	Monitor effective utilisation of the systems at departmental level.
	2.6	Responsible for the compilation and maintenance of departmental manuals and procedures.
	2.7	Liaison between departmental system users and Provincial Treasury.
	2.8	Render a departmental user support (helpdesk) function.

2. PURPOSE OF THE POLICY

The purpose of this policy is to define and outline the roles and responsibilities of the various LOGIS role-players and provide standard guidelines regarding management, access, and usage of LOGIS in Eastern Cape provincial departments. The appropriate implementation and use of LOGIS in the province is critical to ensure that;

- The system is not accessed by unauthorized persons **(confidentiality)**
- information on LOGIS is not altered by unauthorized persons in a way that it is not detectable by authorized users **(integrity)**
- users of LOGIS are the persons who they claim to be **(authentication)**

It is therefore critical that:

- LOGIS is managed and configured in a standard format across all departments in the province, access control is properly managed and access violations timeously identified and reported on.
- A policy is in place to guide and direct access and utilization of the system.
- The roles and responsibilities of the Provincial Support Officials at Provincial Treasury, Departmental LOGIS System Controller and the Departmental users are clarified.
- Standard guidelines are provided on the use of LOGIS.

3. SCOPE

This policy is applicable to all users of LOGIS in all provincial departments in the Eastern Cape Province. These are, but are not limited to:

- Accounting Officers
- Departmental Supply Chain Practitioners
- Programme Managers
- Responsibility Managers
- System Controllers
- Users / Capturers
- Supervisors / Authoriser
- Internal Audit
- Consultants

- Contract Workers
- Auditor General
- Audit Committees
- Service providers

4. DEFINITION OF TERMS

For the purpose of this document, meanings and definitions of terms used in this document are provided below.

"Annexure": A document that is attached to the policy

"BAS": Basic Accounting System

"CFO": Chief Financial Officer

"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

"Function": The task that is allocated to the user

"LOGIS": Logistical Information System. A computerized system that accounts for procurement, inventory and asset management transactions and interfaces with BAS within the department

"LOGIS releases": Enhancements on LOGIS

"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.

"Transversal Systems": BAS, PERSAL and LOGIS

"**User":** An employee/person who has a user ID to access the LOGIS system and should use that access for purposes of capturing, authorizing transactions, updating or amending system data and extracting management information from LOGIS

"User ID": A unique code allocated to a user in order to access the system(s)

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

5. LEGAL FRAMEWORK

This policy document aims to provide a framework within the guiding principles of the following:

5.1 PFMA

Section 18: functions and powers of a provincial treasury

a) ([1] c) A provincial treasury must promote and enforce transparency and effective management in respect of revenue, expenditure, assets and liabilities of provincial departments and provincial public entities;

b) ([2] b) must enforce the Act and any prescribed norms and standards including any prescribed standards of generally recognized Accounting practice (GRAP) and uniform classifications systems, in Provincial Departments."

Section 38 General responsibilities of accounting officers

The accounting officer for a department, trading entity or constitutional institution-

a) must ensure that the department, trading entity or constitutional institution has and maintains-

   i) effective and transparent systems of financial and risk management and internal control, as per Section 38 (1)(a)(i);

   ii) an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective;

b) is responsible for the effective, efficient, economical and transparent use of the resources of the department, trading entity or constitutional institution, as per Section 38(1)(b)

Section 40 Accounting officers' reporting responsibilities

The accounting officer for a department, trading entity or constitutional institution-

c) 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, as per Section 40(1)(a);

6. OVERVIEW OF LOGIS

LOGIS is implemented in each department through the deployment of a “LOGIS Store” per level of transactional responsibility. Therefore, should a department have regional offices that run their own budgets on BAS they will require a separate LOGIS Store per regional office.

LOGIS consists of 3 modules – Procurement Integration Module, Assets Module and Inventories Module.

Table 1: LOGIS Role Players and their Responsibilities

System Controller	
• Maintenance of store-specific data • Interpret and act on system information as generated in the system report • Allocations of LOGIS functions to various users	
Procurement	
Player	***Role***
Cost Center Manager	• The user within a store, and could be a department or an individual • Responsible for approval of Requisitions
Cost Center Officer	• Responsible for compiling consolidated lists of requirements per department • Places requests for stock from the store
Order Officer	• Manually and system approve orders, capture Procurement Advice (PA) • and if needed approve PA
Payment Officer	• Check and capture Supplier Invoices and ensure that payments are correctly made to the relevant Suppliers
Inventory	
Posting/Transit Officer	• Control the receipts and issues of stock into and from the Store • To control the delivery dates of the Suppliers and to communicate any • information regarding damaged goods delivered by Suppliers
Warehouse Officer	• Responsible for the issue and

	receipt of items into and from the Store. • The year-end stocktaking is also part of his/her responsibilities
Asset Management	
Player	***Role***
Asset Manager	• Recording of assets based on acquisition date • Verification of historical Asset data on LOGIS • Annual stock taking
Asset Miscellaneous Officer	• Assistance in annual stock taking • Recording of assets based on acquisition date • Assistance in verification of asset data
Posting/Transit Officer	• Responsible for receiving of assets • Verifies quantity, quality, correctness and delivery criteria of assets received from suppliers • Verifies quantity, quality and correctness of assets to be issued to Cost • Centre Managers

The following user types exist for the LOGIS System:

User Type	***Function***
User Type 1 System Administrator	• Responsible for creating other User Type 1 IDs and User Type 6 IDs. • Responsible for creating/managing User Type 2.
User Type 2 Departmental System Controller	• Limited Enquiry & Report Functionality access • Responsible for creating/managing User Type 3 (System Controller). • Access to all the stores in National Department/Province
User Type 3 Store Specific System Controller	• Responsible for creating/managing 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 Official	• Access to LOGIS Functionality as specified on SASP & BRRR. • Only has access to specific store in the Department they are linked to.
User Type 5 Cost Centre Official	• Access to LOGIS Functionality as specified on SASP & BRRR. • Only has access to specific store in the Department they are linked to.
User Type 6 Special User IDs	• 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 Regional System Controller	• Access to a selection of stores. • Access to enquiries, reports & creation of new User IDs in the stores they have access to. • Must be created and managed by User Type 2.

User Type	***Function***
User Type 8 Departmental Asset/Inventory Manager	• Access to transaction over multiples stores in Department. • Grant of access to stores & functions must be managed by either User • Type 7 with SASP OR User Type 2.

Table 2 – LOGIS User Types and Functions

To successfully maintain LOGIS in a department, one (1) departmental system controller (User Type 7) must be appointed at Head Office per department. However, each LOGIS Store within a department requires its own LOGIS Controller (User Type 3) who has to be correctly appointed and trained. The department must therefore appoint a systems controller per store, who will report to the main system controller.

The User Type 7 can be translated to a User Type 8 if sufficient motivation is provided and approval is obtained from Provincial Treasury. A User Type 3 can be translated to a User Type 4 if sufficient motivation is provided and approval is obtained from Provincial Treasury.

The departmental system controller has overall responsibility for the use of LOGIS in the department. It is essential that all system controllers have sound knowledge of the departmental SCM processes, procedures and requirements. All system controllers must undergo 9 days formal training on the LOGIS Systems Controllers Course (with the pre-requisite of having completed the LOGIS Literacy Course) and must obtain at least a 70% pass-mark in their assessment within 12 months of being appointed.

7. ROLES AND RESPONSIBILITIES

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

7.1 Accounting Officer

The accounting officer or his/her designee in the respective provincial department is responsible for the appointment of a departmental systems controller for LOGIS and to also ensure that prescribed policies and procedures are in place and adhered to.

The Provincial Treasury must form part of the recruitment process of employing a new system controller.

Some of the responsibilities of the Accounting Officer include:

i. Ensure continuity of LOGIS system controller function by appointing a relief departmental system controller in the event of the main system controller being absent from work. Provincial Treasury must be informed in writing before the assumption of duty of the relief departmental system controller.

ii. To ensure that system controller changeover procedures are adhered to, i.e. a substitute LOGIS system controllers/relief system controller completes the necessary LOGIS application forms. Forms must be signed/ authorized by the departmental CFO and forwarded to the Provincial Treasury for actioning to National Treasury. No LOGIS system controllers/relief system controller should be allowed to access LOGIS without following proper changeover procedures.

iii. To implement proper processes for internal control and risk management;

iv. To enforce appropriate disciplinary measures when there are transgressions;

7.2 Provincial LOGIS System Controller

A provincial system controller resides at the Provincial Treasury, and is responsible for the following duties:

i. Create, deactivate and maintain user profiles for EC departmental LOGIS system controllers

ii. Inform all departmental system controllers of significant changes/ enhancements to system functionality and/ or operations

iii. Take responsibility to facilitate the capacitation of provincial users according to their training requirement

iv. Ensure implementation and or re-implementation of LOGIS where necessary is conjunction with CFO's and Departmental SCM Leaders (in conjunction with National Treasury)

v. The Provincial system controller shall receive from the mainframe, RACF reports to monitor access violations, log on violations and group special activities on daily and monthly basis and forward to departmental system controllers for further discrepancy investigation and determining user training requirements

vi. Receive and action original application forms for new LOGIS System Controllers/Relief System Controllers

vii. Ensure that original, new LOGIS System Controllers/Relief System Controllers LOGIS application forms are forwarded to National Treasury (a copy of the application forms must be kept on file at the Provincial Treasury, clearly marked for that purpose).

viii. Implement a generic policy pertaining to access and system security.

ix. Standardize system structures throughout departments to facilitate management information and reporting requirements. All departmental organizational structures to reflect the authorised organogram of the department.

x. Ensure that access to new/current users who have not completed the required formal training in accordance with his/ her profile is limited/ refused.

xi. Perform systems assessments versus training stats on functional areas to which users have access.

xii. Ensure the implementation of effective user account management by system controllers

xiii. Ensure the standardization of user I.Ds to PERSAL numbers.

xiv. Ensure standardized password control The Provincial Treasury recommends that the password length be at least (8) characters.

xv. Ensure standardized password expiry period. Provincial Treasury recommends that the password expiry period be no more than 30 days.

xvi. Ensure standardized password reset period. Provincial Treasury recommends that the password reset period be at least 30 minutes.

xvii. Ensure the deactivation of dormant users in service (within 30 days) as well as users who have left the service (immediately);

xviii. Catalogue/ request specific reports on a monthly basis that require ongoing attention by departments/ institutions (e.g. orders older than 3 months that are open).

xix. Perform quarterly user account management audits of the LOGIS system. Flag deviations/violations and ensure departmental compliance.

xx. Ensure compliance with all National Treasury LOGIS notices and Provincial Treasury LOGIS system policy and notices.

xxi. Perform quarterly assessment of the duties and activities of the departmental system controller(s) to ensure that they are executed in accordance with the prescribed procedures and that the control measures are maintained. User activity reports of system controller(s) to form part of monitoring tool.

xxii. Ensure that system controller(s) complete and provide the Provincial Treasury with a certificate of compliance quarterly. The certificate is to ensure that system controller(s) indicate that:

a) All active users on the LOGIS system are a true reflection of the department's officials, who are permitted access, in accordance with their profiles, on the LOGIS systems.

b) All users who have left the employ of the department have been de-activated on the LOGIS System.

c) All **users** who have been appointed or seconded to other section/directorate/unit/profiles have been amended, to reflect the new office of employ.

7.3 Departmental LOGIS System Controller

The departmental system controller is an official who resides at the department using LOGIS. All system controllers are directly responsible to the departmental CFO. He/she must ensure smooth and appropriate operation of LOGIS in the department. The primary tasks of the system controller are:

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

- Sub LOGIS system controllers.
- A person employed within the public service who is required to work on LOGIS performing functions relevant to their duties
- An internal auditor, who requires enquiry access for auditing purposes.

- A person from the office of the Auditor General who requires enquiry access.
- A contract worker, consultant, casual employee or intern employed by a department who requires access.
- Provincial system controllers who may require specific access to a particular LOGIS Store

b) Deny, terminate or temporarily withdraw a user's access to the LOGIS system if:

- There is suspected misuse of his/her user ID
- There is suspected fraudulent activity
- A user ID is not utilized for a period of 30 days if the system does not automatically deactivate/disable the user account

c) Reset password for users who have been revoked. An **ID Reset form** must be completed by the user and submitted to the LOGIS system Controller, prior to the password being reset.

d) Review all user profiles on a regular basis (quarterly reviews are advisable). System controllers must provide **written confirmation (quarterly)** to the Provincial Treasury, indicating that all active users on the LOGIS system are a true reflection of the department's officials, who are permitted access, in accordance with their profiles, on the respective systems.

e) The LOGIS system controller is responsible for the orientation of new LOGIS users.

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

g) Provide access control for users in the following areas:

- resetting of passwords.

h) Responsible for the maintenance of functions assigned to users according to his/her job descriptions.

i) Detect and investigate any inactive users.

j) Maintain departmental parameters.

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

l) Determine official training requirements and responsible for person-to-person training.

m) Facilitate the clearing of interface exceptions.

n) Jointly responsible for compiling and maintaining a departmental procedure manual

o) To grant users only access to functions relevant to their duties.

p) Monitoring effective use of the LOGIS system.

q) Liaise between departmental users and Provincial Treasury.

r) Act as LOGIS advisor within their department.

s) Lead the implementation of LOGIS in their department

t) Implement and control audit measures.

u) Enforce segregation of duties within the department.

v) The departmental LOGIS system controller also has the ultimate responsibility to ensure that his own user ID and password is safeguarded against unauthorized access. He/she must send an application form for user password reset to Logic call center, National Treasury, whenever a reset of password for his/her own user is required.

Please note that the system controller's responsibilities do not include:

a. Conducting printer and desktop support
b. Administering the Network
c. Maintaining the file and address servers;
d. Installing LOGIS,
e. Executing functional transactions

7.4 LOGIS User/Capturer

LOGIS users are end users of the LOGIS and are responsible:

a) To capture /generate orders on LOGIS.

b) To request LOGIS reports and perform enquires.

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

d) At all times a "Complex password" must be utilised

e) The Provincial Treasury strongly recommends that passwords are changed frequently at least every (30) working days, or immediately when the possibility exists that the password secrecy was compromised.

f) ID's and passwords are solely for the relevant user's access to the systems 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 provincial system controller/ functional managers.

7.5 LOGIS Supervisor/Authorizer

a) To verify and authorize / reject transactions captured on LOGIS.

b) To request LOGIS reports and perform enquires.

8. NEW LOGIS USERS

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 accorded the correct profile on the system.

Should the application indicate that the user has successfully completed the formal training in accordance with his/ her profile, contained in the request; immediate access will be granted to the user. If however the formal training in accordance with the requested profile has not been successfully completed, temporary access for three (3) months will be granted on the following conditions:

- The user undergoes formal training within the three month period;
- The department undertakes to provide system orientation and person-to-person training to the user until such time that the formal training is undertaken.

In practice, it will be expected of the user in consultation with his/ her supervisor to commit via the departmental system controller to specific dates to undergo formal training within the three months period. A confirmation of nomination will be forwarded by Provincial Treasury directly to the user as well as the departmental system controller. If the user fails to attend the course for which he/ she is nominated over a six months period, such user will be de-activated on the system.

If the initial course is attended within the three (3) month's period and the official is found to be "not competent", a further opportunity will be granted to the user to attend the course again, within three (3) months' period to improve competency. If again found to be "not competent" during the next three months, the user will be deactivated on the system.

9. CURRENT LOGIS USERS

It will be expected of all current users that have not undergone formal training, in accordance with their system profiles, to attend such training within three months. This training is provided by the Provincial Treasury. Users, who have had access to a specific profile for a period exceeding two years and have not successfully completed the formal training, will be given the option of attending the formal training or alternatively completing the competency test. If successful, the user will be issued with a certificate of competency. If unsuccessful, the user will be required to complete the formal training and if found to be "not yet competent", will be deactivated on the system.

10. LOGIS USER ACCOUNT MANAGEMENT

Departments should protect their information assets from the risks created by both intentional and unintentional misuse of resources. LOGIS has to be protected from unauthorized use.

Poor access control practices can lead to unauthorized disclosure of confidential information (confidentiality), unauthorized changes to data (integrity) or loss of continuity of business processes (availability). The consequences of not having appropriate access controls in place should be considered in terms of the value of the asset to the organization from both a quantitative and a qualitative perspective, e.g. reputation, public perceptions, regulatory effect and financial effect. Preventive controls should therefore be implemented to minimize these risks to a level that is acceptable to the department. Detective controls are also required to secure the process. Proper user account management is one of the processes that can assist in achieving better information security, responsibility and accountability by performing regular user account reviews.

The following good user account management practices, as recommended by the Auditor General's office, should be implemented to minimize risks associated with improper management of user accounts:

a) User registration.
b) Modification/changes.
c) User deregistration.
d) Review of user access rights
e) Privilege management.
f) User responsibilities.
g) Password usage.
h) Unattended user equipment.
i) User password management.
j) Monitoring of access/user activities.

11. USER ACCOUNT MANAGEMENT PROCEDURES

User account management procedures should cover all stages in the life cycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services. All procedures should be documented and formally approved (signed and communicated). It should also be ensured that access control responsibilities, e.g. access request, access authorization and access administration and monitoring, are segregated throughout the process.

11.1 User Registration

Departments should have formal user registration procedures for granting access to information systems. This procedure should ensure the following, inter alia:

a) A formally documented access request should be completed and be approved by the user's supervisor.

b) The access request form should make provision for adequate details regarding the user, supervisor, and type of access, approvals, etc.

c) Approval from the business/system owner should be obtained before access is granted to business information resources.

d) The level of access granted to users to allow access to information/systems should be appropriate in terms of the business purpose and should be consistent with an organisational security policy, e.g. it should not compromise segregation of duties (duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or abuse of the organization's assets) as follows:

   I. A written statement should be issued to users explaining their access rights.

   II. Users should sign statements indicating that they understand the conditions under which access is granted.

   III. Unique user identifications (IDs) should be created that identify users and link their actions to their IDs.

   IV. Redundant user IDs should not be issued to other users.

11.1.1 Standardise user I.D's to PERSAL number

Currently, system users are given access to the system under more than one user I.D. (undermining segregation of duties). To ensure that segregation of duties is maintained, the PERSAL number must be utilised as the LOGIS user I.D. The only exception being those people who do not receive salaries via PERSAL (e.g. consultants) in which case the first 8 digits of their RSA I.D. number must be used or in the case of a foreigner, the first 8 digits of the passport number.

11.1.2 Standardise password length

Systems in general, provide for a minimum and maximum password length. Users tend to utilise the minimum number of characters and use passwords which are easily identifiable (only numeric or only alphabetical) increasing the risk of irregularities/ fraud. In all instances, the maximum password length provided for (LOGIS currently 8 characters) must be utilised and the password must consist of a combination of numeric and alphabetical characters to limit the possibilities of easy identification.

11.2 Modification/Changes

Changes in user status include changes of job function, roles, responsibilities and transfers within the organization. A procedure should be established to manage these changes in user status and should include, inter alia, the following:

a) Changes should be communicated to information owners, users, superusers, supervisors or any person/department responsible for defining, granting, changing or revoking access privileges.

b) The access rights of users who have changed job function, departments, roles, responsibilities, etc. should immediately be removed or blocked.

c) Procedures for the registration of users should be followed when the status of a user changes.

11.3 User Deregistration

System Controller request System Report on user profiles for all users (which outline all active and inactive users and identify the following:

a) All dormant users from the system within 30 days.

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

c) Terminate all dormant users.

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

11.4 Review of User Access Rights

The review of users' access rights is necessary to maintain effective control over access to data and information services. Users' access rights should therefore be reviewed as follows:

a) At regular intervals, e.g. every six months

b) After any changes such as:

I. Promotion.

II. Demotion.

III. Termination of employment when moving from one section/division to another within the same organization.

c) Authorizations for special privileged access rights should be reviewed at more frequent intervals, e.g. every three months.

d) Privilege allocations should also be reviewed at more frequent intervals to ensure that no unauthorized privileges have been obtained.

e) All changes to privileged accounts should be logged for periodic review.

11.5 Privilege Management

The allocation and use of privileges should be restricted and controlled. Inadequate control of system administration privileges can be a major contributing factor in failures or breaches of systems. A formal authorization process should be used to control the allocation of privileges in multi-user systems that require protection against unauthorized access. The following steps should be considered:

a) The access privileges associated with each system function, e.g. order generation, supplier maintenance etc., as well as the users to which they need to be allocated, should be identified.

b) Privileges should be allocated to users on a need-to-use basis and on an event-by-event basis, i.e. the minimum required for their functional role and only when needed.

c) An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.

d) Changes to privileged accounts should be logged for periodic review.

11.6 LOGIS User Responsibilities

The co-operation of authorized users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

11.6.1 Password Usage

Passwords are a basic control in verifying a user's identity before access is granted to an Information system or a service according to the user's profile. Each employee is responsible for all the actions performed with his/her password, even if it is demonstrated that an action was carried out by another individual using the user's password. Users should therefore follow good security practices in the selection and use of passwords and the following should be kept in mind:

a) Keep passwords confidential.

b) Avoid keeping a record of passwords, e.g. hard copy or electronic file.

c) Change passwords whenever there is any indication of possible system or password compromise.

d) Compose passwords that are:

   i. Easy to remember.

   ii. Of sufficient minimum length, e.g. eight characters.

   iii. Not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, dates of birth, etc.

   iv. Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries)

   v. Free of consecutive, identical, all-numeric or all-alphabetic characters.

   vi. Change passwords at regular intervals or based on the number of times access has been obtained. The passwords for privileged accounts should, however, be changed more frequently than normal passwords.

   vii. Avoid the reuse or cycling of old passwords.

   viii. Change temporary passwords at first logon. Thereafter it must be changed after every expiry period, as set by the systems administrator.

   ix. Never share individual user passwords among users.

11.6.2 Password Management

a) Users reset their own password on Portal according to LOGIS notice 4 of 2014 (System Controllers are not allowed to change the email address of users on IDCI unless the dormain of the department is changed by departmental ICT Management). However, there are instances in the province where there is unreliable connection; in those situations System Controller will reset users on the main frame.

b) The following headings must appear on the reset application form:

i. Name and Surname of the user.
ii. Department/Store number.
iii. User ID, Contact details of the user
iv. Signature of the user and date
v. Name and Surname of the System Controller, date reset.
vi. The password reset application must be complete with a clear copy of the SA ID and must be signed off by the user and the System Controller.
vii. The input document must contain a declaration of secrecy whereby the user attest to being fully responsible for the passwords.

Unattended User Equipment

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities in regard to the implementation of such protection. Users should be advised to, inter alia:

a) Terminate active sessions when finished, unless such sessions can be secured by an appropriate locking mechanism, e.g. a password-protected screen save

b) Log computers off at the end of a session (i.e. it is not sufficient to merely switch off the PC 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.

11.7 Controls on the Allocation of Passwords

The allocation of passwords should be controlled through a formal management process and this process should include the following requirements as a minimum:

a) Users should be required to sign an undertaking to keep personal passwords confidential. This signed statement could also be included in the terms and conditions of employment.

b) If users are required to maintain their own passwords, they should be provided with a secure initial password, which they should be required to change immediately at first logon.

c) Procedures should be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password.

d) A secure procedure should be followed when granting users temporary passwords and the use of unprotected (clear text) electronic mail messages should be avoided.

e) Temporary passwords should be unique and should conform to password standards.

f) Users should acknowledge receipt of passwords.

g) Passwords should never be stored on computer systems in an unprotected form.

h) Default vendor passwords should be replaced as soon as the installation of systems or software has been completed.

11.8 Monitoring of Access and User Activities

A set of controls should be defined for controlling and monitoring user access and activities on system. The following should, inter alia, be considered:

a) Repeated failed login attempts should be identified and investigated.

b) Any blocked or suspended user ID (three or more consecutives failed attempts) should be investigated to verify that the user is the authorized owner of the user ID and not an unauthorized person trying to discover passwords.

c) Inactive users should be monitored and corrective action should be taken after a predefined period of inactivity, e.g. users that have been inactive for 30 days should be blocked.

d) Activity carried out by default users (e.g. guest, administrator, owner and root) should be monitored on a daily basis.

e) Access to critical accounts, log files, data files and databases should be monitored and controlled.

f) Periodically, logs should be reviewed to monitor the activities of privileged users and failed access attempts.

g) The organization should be prepared to react appropriately should a breach of access (such as an unauthorized intrusion) be detected.

h) Periodically, the organization should check for and remove or block redundant user IDs and accounts.

i) The activities of the privileged or super user login account should be closely monitored and reviewed by senior computer security management.

j) User passwords should be reviewed to ensure that an appropriate level of complexity is maintained.

12. GENERAL REQUIREMENTS

a) Any LOGIS user who does not adhere to this policy when using LOGIS or who misuses LOGIS should immediately be deactivated from LOGIS by the departmental system controller, until the departmental investigation into the matter has been finalized. A departmental system controller should only reactivate the user after investigation by the relevant department, which cleared such user of any wrong doing, or as directed by the CFO or Head of Department. A full report of such incidents should be provided to the provincial system controller.

b) Any LOGIS system controller who does not adhere to this policy when using LOGIS or who misuses LOGIS should be immediately deactivated from LOGIS by the provincial system controller. This will be affected by logging a call with the LOGIK call center at the National Treasury requesting the immediate deactivation of the defaulting system controller from LOGIS, until the departmental investigation into the matter has been finalized. The LOGIK call center at the National Treasury should only reactivate the system controller after investigation by the relevant department, which cleared such user of any wrong doing, or as directed by the CFO or Head of Department. A full report of such incidents should be provided to the provincial LOGIS system controller.

13. MONITORING AND EVALUATION

a) The duties of the departmental CFO regarding the departmental system controller(s) include:

i. Familiarizing himself/herself with the duties of the LOGIS system controller.

ii. Regular monitoring of the duties and activities of the departmental system controller(s) to ensure that it is executed in accordance with the prescribed procedures and that the control measures are maintained.

b) The duties of the provincial system controller regarding the departmental system controller(s) include:

i. Monitoring that the departments execute proper access control procedures on a quarterly basis. Receipt of written confirmation from the department that all active users on LOGIS are a true reflection of the departmental users permitted to access the respective system(s).

ii. Performing various security assessments on departmental LOGIS use.

14. 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 policy.

15. IMPLEMENTATION

The implementation of this policy is effective as from the date of the signature. The responsibility for the implementation of the policy rests with the CFO. Risk management component shall review compliance to this policy on an ongoing basis.

16. NON COMPLIANCE

Non-compliance to this policy will be dealt with in-line with public service disciplinary code of conduct. However consequence may include the withdrawal of user accounts, suspension from work, dismissal from public service, or imprisonment depending on the severity of the non-compliance.

17. POLICY REVIEW

This policy shall be reviewed every two years to ensure that it is effective and relevant.

18. COMMUNICATION

The system controller must ensure that this policy is made available in hardcopy to all LOGIS users. It is also available in an electronic version on the Provincial Treasury's website. Should there be questions and/ or issues of interpretation regarding the application of this policy, please contact the FIS unit at the Provincial Treasury.