

WESTERN CAPE EDUCATION DEPARTMENT

LOGISTICAL INFORMATION SYSTEM (LOGIS) USER ACCOUNT MANAGEMENT POLICY

LOGISTICAL INFORMATION SYSTEM (LOGIS) USER ACCOUNT MANAGEMENT POLICY

TABLE OF CONTENTS

| Section: Topic | Page number |
|---|-------------|
| 1. Definitions | 3 |
| 2. Introduction | 3 |
| 3. Applicability of the LOGIS policy | 4 |
| 4. Designation of provincial system controller | 4 |
| 5. Designation of departmental system controller | 4 |
| 6. Segregation of duties | 5 |
| 7. Creating new user identification numbers and user profiles | 5 |
| 8. Amending user profiles | 5 |
| 9. Deregistration of a user identification number and profile when a user resigns or is transferred | 6 |
| 10. Suspension of inactive user profiles | 6 |
| 11. Verification of the validity of system-level access granted to users | 6 |
| 12. User identification and password control | 6 |
| 13. Monitoring by system controller | 7 |
| 14. Compliance | 7 |
| 15. Monitoring by independent party | 7 |
| 16. Dispute resolution | 7 |
| 17. Policy Review | 7 |
| 18. Date of commencement | 7 |

1. DEFINITIONS

In this document, unless the context indicates otherwise,

| | |
|----------------------------------|--|
| "Accounting Officer" | means a person mentioned in section 36 of The Public Finance Management Act 1999 (Act 1 of 1999, as amended by Act 29 of 1999; |
| "Chief Financial Officer" | means the employee designated in terms of Treasury Regulation 2.1.1; |
| "Department" | means the Western Cape Education Department as a government department listed under Schedule 1 of the Public Service Act; |
| "LOGIS" | means the Logistical Information System used by the Department to report on financial transactions; |
| "employee" | means a person employed by the Department; |
| "supervisor" | means an employee with a designation equivalent to or above that of administration officer, or an employee acting in that capacity; |
| "departmental system controller" | means an employee designated on the fixed establishment of the Department to control the general functioning of the LOGIS; |
| "provincial system controller" | means an employee designated on the fixed establishment of the Western Cape Provincial Treasury to control the creation of and amendments to user profiles; |
| "transversal system" | means a system that is used by more than one department in government; |
| "user" | means an employee who has access to the use of the LOGIS; |
| "user identification number" | means a unique identification number allocated to users of the LOGIS; and |
| "password" | means a password in a unique alphanumeric string only known to the user. (A password is traditionally associated with a user identification number to identify and authenticate a user.) |

2. INTRODUCTION

- 2.1 PFMA Section 38 (1)(a)(i): The accounting officer for a department, trading entity or constitutional entity must ensure that the department, trading entity or constitutional institution has and maintains effective, efficient and transparent systems of financial risk management and internal control.
- 2.2 The effectiveness of the overall control environment for the LOGIS depends on the way various controls are applied at the Department. Where the LOGIS System may have

material control weaknesses in its particular environment, the effectiveness of the overall control environment may be impaired and may lead to increased risks.

- 2.3 It is therefore, necessary to issue departmental policy with regard to the general controls over the LOGIS System managed by the Department of National Treasury.
- 2.4 National Treasury has developed the LOGIS portal to serve as a single sign-on platform for LOGIS Web Applications.

3. APPLICABILITY OF THE LOGIS POLICY

The departmental policy contained in this document applies to all system users of the LOGIS System.

4. DESIGNATION OF PROVINCIAL SYSTEM CONTROLLER

- 4.1 The provincial system controller is an official appointed by Provincial Treasury and is assigned to perform the following functions on behalf of the Department:
- Implement a generic policy pertaining to access and system security
 - Standardise system structures throughout departments to facilitate management information and reporting requirements
 - Limit or refuse access to new or current users who have not completed the required formal training in accordance with their profile.
 - Implement effective user account management
 - Standardise user identification numbers to PERSAL number
 - Standardise password length
 - Standardise password expiry date
 - Deactivate dormant users in the service, as well as users who have left the service
 - Ensure that resubmission queues and exceptions are addressed as a matter of urgency
 - Catalogue or request monthly reports that require ongoing attention by departments or institutions (e.g. payments outstanding for more than 30 days)

5. DESIGNATION OF DEPARTMENTAL SYSTEM CONTROLLER

- 5.1 The Chief Financial Officer or his or her delegate shall appoint in writing a system controller and sub-system controller for the LOGIS System utilised by the Department.
- 5.2 The system controller
- a) is responsible for the effective, efficient, economical and transparent use of the system under his or her control (Such responsibilities must form part of an incumbent's job description and performance agreement.);
 - b) must take into account all relevant financial considerations, including issues of priority, regularity and value for money, when system-related proposals affecting the operations of the LOGIS are considered, and, when necessary, bring those considerations to the attention of the Chief Financial Officer or his or her delegate; and
 - c) must Inform the Chief Financial Officer or his or her delegate of any proposed system changes once he or she becomes aware of such changes.
- 5.3 The supervisor is responsible for the quarterly review of the system controller's access to functionalities.

6. SEGREGATION OF DUTIES

- 6.1 Users may have access only to system functionality directly related to the performance of their daily duties. The Director: Procurement Management may grant access to such functions.
- 6.2 Should the need arise for an employee to help out in a section which requires access to system functionalities which differ from those the employee uses daily, the supervisor of that employee must submit an application and a recommendation for the activation of the functions which differ. The written recommendation must clearly state:
- a) the user's name and designation;
 - b) the user's Persal number;
 - c) the daily functions to be performed;
 - d) the reasons for the amendment;
 - e) whether the user will be responsible for processing or authorising transactions; and
 - f) the effective date and expiry date.

7. CREATING NEW USER IDENTIFICATION NUMBERS AND PROFILES

- 7.1 The provincial system controller will create new user identification numbers and user profiles, subject to the receipt of fully completed and approved LOGIS user request forms, signed by the user's director and duly authorized by the Director: Procurement Management (Annexures A and B).
- 7.2 The following must be provided on the user request form:
- a) The user's name and designation
 - b) The user's Persal number
 - c) The user's identification number
 - d) The daily functions to be performed
 - e) Reasons for the creation of the new user identification number and user profile
 - f) Whether the user will be responsible for processing or authorising transactions
 - g) The activation date
- 7.2 It is important to note that before functions on LOGIS can be allocated to an employee, that employee must have either received the necessary formal LOGIS training from the Provincial Treasury or acquired the necessary experience in LOGIS. An additional prerequisite is that these functions must be in line with the applicant's job description. Applicants not complying with these requirements will not be considered.
- 7.3 The provincial system controller must create the necessary user profile and group functionalities allocations after approval is received from the Chief Financial Officer or his/her delegate.

8. AMENDING USER PROFILES

- 8.1 The provincial system controller will:
- a) amend user profiles only on receipt of a completed LOGIS amendment form approved by the Director: Procurement Management for that particular user (Annexure A and B); and
 - b) allocate amended functions to a user only on receipt of a written motivation from the user's supervisor stating:
 - i) the user's name and designation,
 - ii) the user's Persal number,
 - iii) the user's identity number,
 - iv) the user's daily functions to be performed,
 - v) the reasons for the amendment,

- vi) whether the user will be responsible for processing or authorising transactions,
- vii) the effective date and expiry date.

9. DEREGISTRATION OF USER IDENTIFICATION NUMBER AND PROFILE WHEN A USER RESIGNS OR IS TRANSFERRED

- 9.1 The relevant director shall, as soon as he or she becomes aware of an employee's intention to resign or impending transfer, instruct the departmental system controller in writing to remove the employee's user profile from the relevant system by completing the prescribed user amendment/deletion form. The provincial system controller will be informed in writing to delete the employee's user profile from the LOGIS.
- 9.2 The departmental system controller must ensure that user's profile is removed on the date the employee is transferred or leaves the employment of the Department.

10. SUSPENSION OF INACTIVE USER PROFILES

- 10.1 Depending on the sensitivity of the access granted to a user, the system controller must deactivate user profiles that have been inactive or revoked for a period of three months (90 days).
- 10.2 The Director: Procurement Management will be supplied with a report of inactive and revoked users and must be informed in writing of such changes to the users' profiles. This will be done with the quarterly review of the management and maintenance of user accounts on the Logistical Information System.
- 10.3 The departmental system controller will keep documentation that will serve as evidence that monthly reviews of inactive and revoked user profiles are performed.

11. VERIFICATION OF THE VALIDITY OF SYSTEM-LEVEL ACCESS GRANTED TO USERS

- 11.1 The departmental system controller must perform a check each financial year to confirm that each user's current access is aligned with their job responsibilities. Where any discrepancies are detected, the departmental system controller must immediately inform the supervisor in writing of the discrepancy, and recommend corrective measures for his or her approval.
- 11.2 Users who were allocated incompatible functions must have their access reviewed monthly.
- 11.3 The departmental system controller will keep documentation that will serve as evidence that the periodic reviews were performed.

12. USER IDENTIFICATION AND PASSWORD CONTROL

- 12.1 Users may not make available their user identification numbers and passwords to any other employee or person.
- 12.2 A user who suspects that their user identification number and password have become known to another employee or person, must immediately change their password or request the departmental system controller to change it.
- 12.3 A user's password will only be reset on receipt of a fully completed and signed LOGIS password resetting request form from the supervisor of the user concerned. All user profiles are linked to the departmental system controller's email address, who will be responsible for the resets of passwords for all users.

- 12.4 Passwords should expire automatically after 30 working days and the system should prompt the user to enter a new password.
- 12.5 A user identification number will be revoked after 3 unsuccessful attempts.
- 12.6 Passwords must consist of six (6) to eight (8) characters in length and be alphanumeric.

13. MONITORING BY SYSTEM CONTROLLER

- 13.1 The departmental system controller will request quarterly reports on all users and reconcile them with a report from Provincial Treasury (RACF) on persons who have left the Department. This must be done to ensure that all users on the LOGIS System are still employees of the Department.
- 13.2 A review of the functions allocated to users shall also be conducted quarterly by the departmental system controller. Any changes in function must be approved by the supervisor of the relevant official, documented and communicated to all affected parties.
- 13.3 The departmental system controller will keep documentation that will serve as evidence that the periodic reviews are performed.

14. COMPLIANCE

- 14.1 The departmental system controller, users of LOGIS and line functionaries must comply with the departmental policy contained in this document.
- 14.2 Disciplinary action may be taken if the users are found not to comply with the requirements of this policy.

15. MONITORING BY INDEPENDENT PARTY

- 15.1 An independent party (Provincial Treasury and Auditor-General) will carry out a review of the activities of the LOGIS.

16. DISPUTE RESOLUTION

- 16.1 In the event of any dispute about the interpretation or application of this policy, any party may refer the matter to the Chief Financial Officer or his/her delegate for resolution.
- 16.2 Where the Chief Financial Officer is party to the dispute, the matter may be referred to the Accounting Officer for intervention.

17. POLICY REVIEW

- 17.1 The terms and provision of the policy will be reviewed as and when required.

18. DATE OF COMMENCEMENT

- 18.1 The departmental policy contained in this document takes effect on the day of approval by the Accounting Officer and repeals any other policy in this regard.