Department:
Social Development
NORTHERN CAPE

Mimosa Complex
Barkly Road
Homestead
Private Bag X5042
KIMBERLEY
8300
Tel.: 053-874 9100
Fax.: 0866 309 708
E-mail:scrouch@ncpg.gov.za

Enquiries : Ms. E. Summers
Dipatlisiso :
Imibuzo :
Navrae :

Reference : H2.8.2.2
Tshupelo :
Isalathiso :
Verwysings :

Date : 2013/06/21
Lethla :
Umhla :
Datum :

Ms. C.M. Chotelo
MEC for Social Development
Private Bag x 6110
Kimberley
8300

ADOPTION AND IMPLEMENTATION OF THE DEPARTMENTAL LOGIS SECURITY POLICY

Attached for your consideration and approval by your good self, the departmental LOGIS Security Policy, which has gone through the relevant consultative process.

The Department Social Development's LOGIS Security Policy serves the purpose of ensuring that proper security measures are in place and that users adhere to these measures.

.....

Ms. E. Botes

Head of Department: Social Development

Recommend/not recommend

Date: 21/06/2013

Approval

The LOGIS Security Policy for the Department of Social Development is approved by the Member of the Executive Council and shall come into effect from date of approval thereof.

.....

28/06/2013

C.M.CHOTELO (MPL)

DATE

Member of the Executive Council for Social Development

social development

Department:
Social Development
NORTHERN CAPE

NORTHERN CAPE

DEPARTMENT OF SOCIAL DEVELOPMENT

LOGIS Security Policy

TABLE OF CONTENTS

1. GENERAL

The Department Social Development's LOGIS Security Policy serves the purpose of ensuring that proper security measures are in place and that users adhere to these measurers. The Department's LOGIS Security Policy must be read in conjunction with the following security related documents:

- Security Manual and the LOGIS Literacy Manual published on the LOGIS web site (Security Manual = Procedures / Business Support / Functional / Security Manual)
- LOGIS Literacy Manual (Training / Training Manuals / Search per role player / LOGIS Literacy).
- LOGIS Notice No 4 of 2012 (Publications / Notices / 2012 / June).
- Auditor General Guidelines published on the web site of the Auditor General.

2. LOGIS SYSTEM SECURITY

The following will align the current security measurers regarding users' access to LOGIS with the guidelines issued by the Auditor General.

2.1 THE LOGIS SYSTEM

LOGIS is a Logistical Information System that aims to provide Government with a fair, equitable, transparent and cost effective supply chain and asset management system. LOGIS operations are regarded as economical, effective and efficient.

2.2. USER RESPONSIBILITIES

- Each official/user is responsible and accountable for all activities performed on their signed User-IDs.
- Officials/users may not:
    - Supply colleagues with their User-IDs and passwords – not even the supervisor, manager, senior manager of chief financial officer.
- If it is suspected that someone else might know a password, change the password immediately.
- Password must be changed immediately after the default password is supplied.
- Officials/users are to log off when leaving their desks – even for a short while.

2.3. LOGIS PASSWORD MAINTENANCE

Officials/users may never exchange passwords.

No official/user is allowed use the LOGIS security profile of another official/user.

The Senior Manager: Supply Chain Management and LOGIS System Controllers are to advocate this security measure.

It is a direct breach of the LOGIS security policy if one official/user in the LOGIS environment makes use of the security profile and passwords of other officials/users to execute LOGIS functions.

If this security policy is breached, disciplinary action shall be instituted against transgressing official(s)/user(s).

2.3.1. User-ID: First LOGIS Sign-On Screen

The LOGIS System- or Sub-System Controller receives User-IDs from LOGIK and communicate it to the relevant user(s).

The User-ID consists of three (3) alphabetical (the billing code) and three (3) numerical digits e.g. VJ6.

2.3.2. Password Rules – First Sign-On LOGIS Screen

The new password cannot be the same as the previous 24 passwords used.

The new password must be between six (6) and eight (8) digits.

Ensure password are not based on anything somebody else could easily guess or obtain using person-related information e.g. names, telephone numbers, dates of birth.

Password may not be vulnerable to dictionary attacks i.e. do not consist of words included in dictionaries.

Password must be free of consecutive or identical characters e.g. QWERTY of AAAAAA).

The password must contain at least one (1) numeric and one (1) alpha character; passwords must be free of all-numerical or all-alphabetic characters.

2.3.3 Password Expiry – First Sign-On LOGIS Screen

Users' unique passwords expire every 30 days.

2.3.3.1 Pro-Active Change of Password – First Sign-On LOGIS Screen

Type the User-ID and password, but do not press "Enter".

Tab to the "New Password" field.

Type the unique password followed by "Enter".

A message will be displayed that the new unique password must be confirmed.

Type the new password for a second time, press "enter" followed by "F4".

The password is then changed.

2.3.3.2 Change of Password after Expiry – First Sign-On LOGIS Screen

Type the User-ID and password and press "Enter".

A message will indicate that the current password has expired.

Type the new unique password in the field "New Password" and press "Enter".

The system will prompt for confirmation of the new password.

Type the new password for a second time, press "enter" followed by "F4".

The password is then changed.

2.3.4 Revoked Passwords – First Sign-On LOGIS Screen

It is important to type the unique password correctly. A User-ID will be revoked if the password was typed incorrectly thrice consecutively.

Should User-ID be revoked, the System- or Sub-System Controller is to contact LOGIK to reset the User-ID.

When a user logs on to the LOGIS Mainframe for the first time or after LOGIK has reset a User-ID, the password will be the same as the User-ID e.g.:

For User-ID VJ6010 – VJ6010 should be typed in at both the User-ID and Password fields on the first Sign-On LOGIS screen.

Press "Enter".

The LOGIS system will them prompt the user to type his/her fresh unique password. The user will also be prompt to confirm the fresh unique password.

2.3.5 Second LOGIS Sign-On Screen

The LOGIS System Controller allocates the User-ID – the official/user's PERSAL number – on selection SASP System Administration – Security Profiles).

The password will be revoked if it is typed incorrectly thrice consecutively. The LOGIS System Controller must then reset the password.

The official/user may change the password after it has expired or as often as deemed necessary.

If the password has expired, LOGIS will automatically activate a pop-up window where the password can be changed.

Should the user wants to change the password pro-actively the "Change Password" field must be used.

A "Y" is typed in the "Change Password" field, followed by "Enter" to change the password pro-actively.

2.3.6 Change of Password – Second Logis Sign-On LOGIS Screen

A pop-up window will appear if the password has expired of after "Y" has been typed in the "Change Password" field followed by "Enter".

The new unique passsword is typed in the "New Password" field and "Enter" is pressed.

LOGIS will prompt the official/user to confirm the password.

After the official/user has confirmed the password "Enter" is pressed followed by "F4".

Password is then changed.

2.3.7 Password Rules – Second Sign-On LOGIS Screen

Password is valid for 60 days.

The new password must be a minimum of eight (8) digits.

Password must contain at least one (1) numeric and one (1) alpha character.

Password must contain a caps and small letter.

The new password cannot be the same as the previous 24 passwords used.

Password revoked after 90 days inactivity.

From the 7th day before the password expiry date the official/user will receive a countdown message prompting a password change.

2.4. LOGIS USER TYPES

2.4.1.LOGIS designed in such a manner that clear segregation of duties were built into the system as to ensure that only one function is performed by an official/user. Multiple consecutive functions for one official/user are not allowed.
Various User Types are created on LOGIS not only to ensure clear segregation of duties, but also to ensure that each User-ID is aligned with a particular official/user's job description. Functions allocated to an official/user will be determined by the supervisor in order for the LOGIS System Controller to create a security profile with specific functions for a particular official/user.

2.4.2. The following user types are available on LOGIS:

2.4.2.1. User Type 1 – National Treasury (LOGIK).

2.4.2.2. User Type 2 – Provincial System Controller at Northern Cape Provincial Treasury (NCPT). The Provincial System Controller will always be an Administrative User, created and maintained by National Treasury. The provincial System Controller is responsible for the creation of user types 3, 7 & 8 at provincial departments.

2.4.2.3. User Type 3 – Departmental System Controller. This User is created and maintained by User Type 2 and / or User Type 7. The Departmental System Controller may only have Administrative access to LOGIS. If this user has to perform certain system functions on LOGIS, a type 4 profile must be created to obtain functional access, **but the persal number cannot be used again as a user ID** on selection SASP. A temporary ID (persal number) must be created for a System Controller's LOGIS functions.

2.4.2.4. User Type 4 – Users (SCM, Asset Management & Finance officials). Will be created and maintained by the User Type 3 and will only have Functional access to certain LOGIS selections.

2.4.2.5. User Type 5 – Automated Cost Centre (Cost Centre Clerk & Manager / Authorizer). Will be created and maintained by the User Type 3 and will only have Functional access to certain selections. The Department Social Development is not yet ate the stage where Cost Centres are automated.

2.4.2.6. User Type 6 – National Treasury.

2.4.2.7. User Type 7 – As indicated above, this user will be created by the User Type 2 and will only have Administrative access to LOGIS. Type 7 users may also have access to multiple stores with coupled responsibilities e.g. a sub-system controller at a department's provincial office may have access to the district offices. The User Type 2 will determine to which stores the user type 7 may have access with / without selection SASP and / or IDCI and BRRR. In the instance of Department Social Development the sub-system controller at provincial office has access to all districts' stores, but only for the running of reports and downloading of other management information i.e. to selection BRRR.

2.4.2.8. User Type 8 – This user is created / maintained by the User Type 3 or 7 and will have functional access to multiple stores. Department Social Development does not have a User Type 8.

2.5. LOGIS SECURITY PROFILE (LSP) FORMS

The following LSP forms must be utilized for user account management:

2.5.1. LSP-1: LOGIS USER ID APPLICATION FORM

Form LSP-1 serves as input document for actions to be performed by officials at the LOGIS Support and Administration Unit at Northern Cape Provincial Treasury (NCPT).

Prospective LOGIS user and supervisor must complete and duly sign form LSP-1 and submit to NCPT.

NCPT LOGIS Team creates the Departmental System Controller (User Type 3) or User Type 7.

In the case of System Controllers, the original signed appointing letter must be attached to this form and forwarded to NCPT LOGIS Support and Administration.

Form LSP-1 is also submitted to the Departmental System Controller in order to create User Types 4 & 5. A copy of the job description of users should accompany the abovementioned form to ensure the LOGIS functions are aligned with the official/user's job description.

The role and functions of an official/user as per the applicable job description will determine to which areas, access should be given e.g. LOGIS (second sign-on screen), Corporate Reference Data (CRD), Procurement Integration (PI), F1 – Help, LOGIS Business Information System (LBIS) and Vulindlela. Access areas must be indicated on form LSP-1.

2.5.2 LSP-2: USER PROFILE MAINTENANCE FORM

Form LSP-2 serves as an application to obtain access to or to remove certain selections indicated on the attachment "Selections to be allocated/modified" to the LOGIS System Controller.

User Types 4 submit a completed and duly signed form LSP-2 as well as the attachment "Selections to be allocated / modified" to the LOGIS System Controller.

After creation of a security profile and allocating/removing selections on selection SASP, the System Controller must print report RR121 – Security User Profile Report, per profile and explain the purpose of selections and functions allocated to an official/user's security profile and sign the report. The type 4 user must also sign the report RR121 as confirmation that the allocated selections were explained. Same applies when selections were and removed from a user's security profile. Refer to sub-paragraph 3.2.3.

2.5.3 LSP-3: LOGIS SYSTEM CONTROLLER PASSWORD RESET FORM

Form LSP-3 is submitted by User Types 3 & 7 & to the NCPT LOGIS Support and Administration to reset the LOGIS second screen password if it is not possible to reset the password automatically. The form must be signed by the Chief Financial Officer (CFO) or delegated official or the Head of the District Office in the case of a System Controller. Reasons for resetting the password must be provided e.g. when the system controller returned from annual leave.

Note:

Resetting of mainframe and PI passwords can only be done by National Treasury if it's not possible for a user to reset the password when prompt by LOGIS after 30 days.

2.5.4. LSP-4: LOGIS USER PASSWORD RESET FORM

User Type 4 complete the LSP-4 form for submission to the System Controller to reset the 2nd sign-on LOGIS screen If it was not possible for the user to reset the 2nd sign-on LOGIS screen's password. Reasons for requesting the password reset must be provided.

Resetting of mainframe and PI passwords can only be done by National Treasury if it is not possible for a user to reset the password when prompted by the LOGIS after 30 days.

2.5.5. LSP-5: HANDING OVER OF SYSTEM CONTROLLER FUNCTIONS

Acting (Relief) System Controllers must be appointed in writing by the CFO when the system controller goes on annual leave or when absent. The signed letter and signed LSP-5 form must be forwarded to the NCPT LOGIS Support and Administration to purge the security profile of the current System Controller and to add the new System Controller.

When the System Controller returns from leave same procedures must be followed inform NCPTs LOGIS Support and Administration. The letter as well as the signed LSP-5 must again be forwarded to NCPT that will update the security profiles according to written instructions.

When a system controller is absent and cannot sign the LSP-5 form, it must be mentioned in the letter signed by the designated acting System Controller and CFO.

The duly signed letter and LSP-5 form is submitted to NCPT LOGIS Support and Administration for action. NCPT LOGIS Support and Administration When done will advise the Department *via* e-mail.

3. USER ACCOUNT MANAGEMENT

3.1. SYSTEM / SUB-SYSTEM (RELIEF) CONTROLLER

3.1.1. APPOINTMENT

- The CFO is responsible for the appointment of a System Controller or Acting (Relief) and Sub-System Controllers for LOGIS.
- Only a government official may perform the role of a system controller. Section 44 of the PFMA has reference.
- The CFO is to ensure that the prescribed policies and procedures relating to LOGIS access control are in place and complied with.
    - System Controller / Sub-System (Relief) Controller at Provincial Office: must be appointed in writing by the CFO.
    - System Controller Sub-System (Relief) Controller at District Offices: must be appointed in writing by the District Director.

3.1.2. REGISTRATION ON REMEDY AT LOGIK

The NCPT LOGIS Support and Administration registered Department Social Development's System- and Sub-System Controller on Remedy at National Treasury to be able to log requests at LOGIK. The applicable application form (System Controller Information), published on the LOGIS web site was utilized for this purpose.

3.1.3. REQUESTING GATEKEEPER ID

The NCPT LOGIS Support and Administration will complete and mail the Gatekeeper User ID application form (email template published on the LOGIS web), to the LOGIK Contact Centre to create a gatekeeper ID for each System Controller. The form can be found under Contact Centre / Forms / Gatekeeper User-ID E-Mail form on the LOGIS web site.

3.1.4. CREATING USER SECURITY PROFILE: SASP

System Controllers (user types 3 or 7) must have access to all the selections to be able to:

1. Allocate these selections / actions to personnel;
2. Verify transactions performed by SCM, Asset Management & Finance personnel to assist when experiencing functional problems.

Although allocating all the selections to a System Controller, it will not be possible for a System Controller to perform all the functions due to segregation of duties on LOGIS. The LOGIS System Controller in the Department Social Development only create officials/users' security profiles.

3.2 OTHER OFFICIALS – USER TYPES 4, 5 & 8.

3.2.1 .REQUESTING RACF (MAINFRAME) USER ID'S

RACF ID's will be requested by the User Type's 3 and/or 7 on selection IDCI.

Requests for an ID on selection IDCI take up to three (3) working days for the RACF ID to be active. The request goes *via* National Treasury (LOGIK) to SITA for activation. The status of the request can be viewed online on selection IDCI.

The External Reference Number should be utilized to keep track of users created per store and for filing purposes. This number should start at 1/ for each financial year e.g. 1/2013/14.

RACF / Mainframe user ID's previously utilized by other officials may not be allocated to another person and must be discontinued on selection IDCI.

3.2.2. REQUESTING GATEKEEPER ID'S

In the Department Social Development the Sub-System Controller is responsible for submission of Gatekeeper User ID application forms for user types 4 to the LOGIK Contact Centre.

The application form can be found under Contact Centre / Forms / Gatekeeper User-ID Form or Gatekeeper User-ID E-Mail form. The completed form can either be printed and faxed or e-mailed to the LOGIK Contact Centre.

Officials responsible for Asset Management, or reconciliation of all purchases done pertaining to assets and inventory, requires access to facilities such as LBIS & Vulindlela in order to obtain credible financial information from LOGIS.

Written requests (LSP-1 form) should be submitted to the Manager of Supply Chain Management and in turn submitted to the System Controller to submit these requests to National Treasury (LOGIK) for access.

3.2.3 .CREATING USER SECURITY PROFILE: SASP – USER TYPE 4

Security profiles created for user types 4 must be aligned with their job descriptions. System Controllers must print report RR121 and explain the functions allocated to each person. Users must then sign report RR121 indicating that they understand the conditions under which access is granted.

Refer to sub-paragraph 2.5.2.

4. MODIFICATIONS

The necessary LSP forms should be available as proof for each modification / change.

5. DEREGISTRATION

5.1 RACF (MAINFRAME) ID'S

Online verification of RACF (Mainframe) ID's can be done on selections IDCI. Access rights of users who have left the department or users who are no longer part of Supply Chain / Asset Management should immediately be removed. Deregistration of RACF ID's must be done at least once a quarter.

5.2. GATEKEEPER USER ID'S

National Treasury will forward information regarding gatekeeper user ID's on a monthly basis. Information must be verified and a request should be logged at LOGIK to deregister inactive ID's. Updating gatekeeper ID information must be done at least once a quarter.

6. MONITORING ACCESS RIGHTS, USER ACTIVITIES & PROFILES

6.1. Profiles do not change on a regular basis but to comply with guidelines published in the Good Practice Guide of the Auditor General, profiles of the user types 4 must be verified by the LOGIS sub-system controller in the Department Social Development.

Run report RR121 per quarter for certain profiles to verify if the selections allocated to a profile is still aligned with the job description. This report must be kept as proof that certain profiles have been verified during that quarter. All the profiles must be verified at least once a year

6.2. The Chief Financial Officer is to ensure that:

- The System Controller followed the prescribed processes with the creation and maintenance of user profiles and ID's.
- The supervisor should verify whether requests for access to the system are accompanied by a written approved request, either by the user's manager or supervisor, along with the relevant LSP forms attached to such a request. Refer to paragraph 2.5.
- A copy of the job description of users should accompany the abovementioned form to ensure the functions allocated to the user, is in line with their job description. Report RR121 can be printed and utilized for this purpose. Any discrepancies should be investigated and corrected.
- The System Controller should ensure that a proper filing system is in place where formal written requests for access to the system as well as the applicable requesting forms are attached and filed per user. All these documents should be easily accessible to both the System Controller, the supervisor, the NCPT LOGIS Support and Administration, Internal Audit and the Office of the Auditor General to be scrutinized and reviewed.

6.3. Security Reports available

The following reports can be printed to verify certain information:

- **Report RR121 – Security User Profile Report**: is utilized to provide a System Controller of a site with a list of all the user profiles created on selection SASP. Functions allocated to each user, will be displayed on the second part of this report. Such report should be requested at least once per quarter or if needed for reporting purposes. Only the System and Sub-System Controller should have access to request such a report.
- **Report RR122 – User Profile History Report**. Maintenance done on profiles will display on this report. Supporting documents must be available and filed in sequence of the history on this report. This report should be requested at least once per quarter or if needed for verification purposes. Only the System and Sub-System Controller should have access to request such a report.
- **Report RR123 – Verify RACF ID's.** This report can be requested once a quarter and will list all the RACF ID's requested for each store. Incorrect information must be rectified by the Sub-System Controller. Refer to paragraph 5.1 *supra.*
- **Report RR124 – RACF ID History.** Will display the status and history of RACF ID's and must be printed and verified by the Sub-System Controller on a quarterly basis.

Reports printed must be kept as proof that information has been verified / updated during that quarter.