

social development

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 :
Dipatlisiso :
Imibuzo :
Navrae :
Reference :
Tshupelo :
Isalathiso :
Verwysings:

Ms. E. Summers

H2.8.2.2

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

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

ADOPTION AND IMPLEMENTATION OF THE DEPARTMENTAL NETWORK ACCESS POLICY AND USER ACCOUNT PROCEDURES

Attached for your consideration and approval by your good self, the departmental Network Access Policy and user account procedures, which has gone through the relevant consultative process.

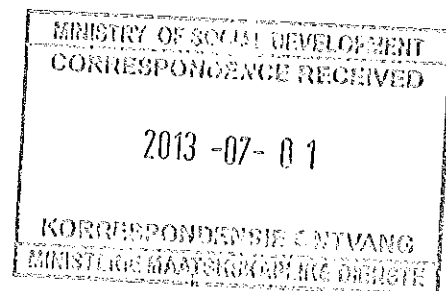
The purpose of the policy is to prevent unauthorised user access to the Department of Social Development's information, through deployment of user account and password management processes.

Ms. E. Botes

Head of Department: Social Development

Recommend/not recommend

Date: 2013/06/27



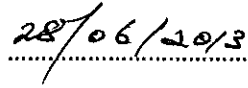
Approval

The Network Access Policy and User Account Procedures 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.



C.M.CHOTELO (MPL)

Member of the Executive Council for Social Development



DATE



social development

Department:
Social Development
NORTHERN CAPE

NORTHERN CAPE
DEPARTMENT OF SOCIAL DEVELOPMENT

**Network Access Policy
and User Account Procedures**



TABLE OF CONTENT

1. Purpose	3
2. Scope	3
3. Policy Details	3
4. Enforcement	7
5. Recommendation	7

1. Purpose

To prevent unauthorised user access to department of Social Development information through deployment of user account and password management processes.

Procedures 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 and network. All procedures are documented and formally approved (signed and communicated)

2. Scope

This document defines the policy required to securely deploy, manage and control user accounts and passwords. Accounts and passwords are the primary security credentials used to identify, authenticate and authorize access to Department of Social Development ICT systems.

The policy applies to all Social Development ICT users (e.g. employees, officers, staff, consultants, interns) of systems, applications and networks.

3. Policy Details

3.1. Requirements for system access

Access to ICT services and associated data will be controlled on the basis of business requirements.

Service providers (both internal and external) must be given a clear statement of the security requirements for system access in order to implement and maintain an effective level of control of access to information services and data.

- The information security requirements of the application;
- Conformance to relevant legislation as well as any contractual obligations regarding protection of access to data or services;
- Standard user access roles.
- A schedule of when access rights need to be reviewed.

3.2. User Registration

A formally documented access request must be completed and be approved by the user's Supervisor.

- The access request form must make provision for adequate details regarding the user.
- Approval from the relevant system owner's shall be obtained before access is granted to Social Development information resources.
- The level of access granted to information and 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 misuse of the organisation's assets).

- Unique user identifications (IDs) should be created that identify users and link their actions to their IDs.
- Redundant user IDs shall not be issued to other users.

3.3. Modification / Changes

Changes in user status include changes of job function, roles, responsibilities and transfers within the organisation.

- Changes must be communicated to information owners, users, supervisors or any person/department responsible for defining, granting, changing or revoking access privileges.
- The access rights of users who have changed job function, roles, responsibilities, etc. should immediately be removed or blocked.
- Procedures as for the registration of users should be followed when the status of a user changes.

3.4. User deregistration

The access rights of users who have left the organisation must immediately be removed.

3.5. 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:

- At regular intervals, 1 x per Quarter
- After any changes such as:
 - promotion
 - demotion
 - termination of employment
- When moving from one section/division to another within the same organisation

3.6. Monitoring of user Access / User Activities

The following controls are defined for controlling and monitoring user access to and activities on systems.

The following is considered:

- Repeated failed login attempts identified and investigated.
- Any blocked or suspended user ID (three or more consecutive failed attempts) investigated to verify that the user is the authorised owner of the user ID and not an unauthorised person trying to discover passwords.
- Inactive users will be monitored and corrective action taken after a predefined period of inactivity, Users that have been inactive for 60 days will be blocked.
- Activity carried out by default users (e.g. guest, administrator, owner and root) will be monitored on a daily basis.
- Access to critical accounts, log files, data files and databases will be monitored.

- Periodically, logs will be reviewed to monitor the activities of privileged users and failed access attempts.
- The organisation will be prepared to react appropriately should a breach of access such as an unauthorised intrusion be detected.
- Periodically, the organisation will check for and remove or block redundant user IDs and accounts.
- The activities of the privileged login accounts will be closely monitored and reviewed by the Government Information Technology Officer (GITO).
- Users' passwords should be reviewed to ensure that an appropriate level of complexity is maintained.

3.7. User Responsibilities

The cooperation of authorised users is essential for effective security.

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 authorisations.

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 must therefore follow good security practices in the selection and use of passwords and the following should be kept in mind:

- Keep passwords confidential.
- Avoid keeping a record of passwords, e.g. hard copy or electronic file.
- Change passwords whenever there is any indication of possible system or password compromise.
- Compose passwords that are:
 - easy to remember
 - of sufficient minimum length, e.g. six characters not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, dates of birth, etc.
 - not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries)
 - free of consecutive, identical, all-numeric or all-alphabetic characters.
- 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.
- Avoid the reuse or cycling of old passwords.
- Change temporary passwords at first logon.
- Never share individual user passwords among users.

All users must:

- terminate active sessions when finished, unless such sessions can be secured by an appropriate locking mechanism, e.g. a password-protected screen saver
- log computers off at the end of a session (i.e. it is not sufficient to merely switch off the PC screen or terminal)
- secure computers from unauthorised use by means of a key lock or an equivalent control ,e.g. password access, when not in use.

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

- Users shall 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.
- If users are required to maintain their own passwords, they shall be provided with a secure initial password, which they should be required to change immediately at first logon.
- Procedures shall be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password.
- A secure procedure shall be followed when granting users temporary passwords and the use of unprotected (clear text) electronic mail messages should be avoided.
- Temporary passwords shall be unique and should conform to password standards.
- Users shall acknowledge receipt of passwords.
- Passwords must never be stored on computer systems in an unprotected form.
- Default vendor passwords must be replaced as soon as the installation of systems or software has been completed.

Passwords for emergency privileges must be lodged in a safe and secure location and accessed only in accordance with authorised procedures.

The use of emergency systems administrative accounts, set up in advance for emergency access, must be controlled; e.g. store super user IDs in a sealed envelope in a secure location such as a safe, together with a list of people permitted access in an emergency. The sealed envelope shall contain details of the systems administrator to be contacted if used. This will ensure that a new sealed envelope with privileged account information is provided.

Any actions taken during an emergency must be accurately recorded.

An effective password management system will be used.

The department's password management system falls by the provincial Information Technology Unit for the Novell Netware and Groupwise system. BAS, PERSAL, LOGIS and NISIS will use their password management systems as provided by National Department of Social Development:

- Enforce the use of individual passwords to maintain accountability;
- Require users to select and change their own password and include a confirmation procedure to allow for typing errors;
- Ensure passwords conform to the Department of Social Development's minimum standard by exposing them to a utility such as "crack" or similar;
- Enforce individual password changes every three months or at earlier intervals whenever:
 - an audit identifies that a password has been used which does not conform to the standard; or
 - system tools compromise a password, or
 - a user suspects that their password has been compromised; or
 - the system owner has specified more frequent password changes due to the sensitivity of the system or information being accessed.
- Enforce Generic Network Account password changes for network connected systems (and standalone systems providing access to information classified as Confidential or higher) at intervals of 60 days or whenever personnel changes occur;
- Enforce password changes for systems administrative accounts, e.g. those with access to system utilities, every 30 days;
- Maintain a record of previous user passwords for 12 months, and prevent users from reusing them;
- Not display passwords on the screen when being entered;
- Prevent new staff from inheriting User IDs and passwords from their predecessors;
- Log password reset requests, keeping details including the User ID (for which the password was reset), the name of the resetting staff member and the time the reset was initiated.
- Ensure passwords reuse is not permitted within 12 months or 12 iterations;
- Alter default vendor passwords (and IDs if possible) following installation of software.
- Disable user access of all permanent staff, contractors or consultants immediately after they leave.

4. Enforcement

Any employee found to have violated this policy will be subject to appropriate disciplinary action.

5. Recommendation

It is recommended that the MEC approves the Network Access Policy and User Account Procedure to protect and secure the department's ICT infrastructure.