LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

User Access Management Policy

Ref: 6/1/P

Date of effect: 13 June 2016

Recommended:

M Maisela

Head of Department

(Maisela, RJ)

03/06/2016

Date

Approved:

MEC for Agriculture and Rural Development:

(Matshoge, BAJ)

13/06/16

Date

Table of Contents

1. Acronyms and abbreviations

GITO	Government Information Technology Office
HOD	Head of Department
IT	Information Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Council
SITA	State Information Technology Agency

2. Executive summary

The User Access management Policy aims to cover all matters relevant to the management of user access within the IT system of the LDARD. The SITA standards are described in length, granting of access and user rights as well as the management of passwords and audit trials are discussed and explained. Roles and responsibilities are set out and monitoring is discussed.

3. Introduction

The access control requirements and standards aim is to ensure that computer resources and the integrity of data are protected at all times. Since user profiles are regarded as electronic signatures as outlined in the Electronic Communication and Transaction Act. Act 25 of 2002. This procedure is intended to ensure that:

I) Only authorized individuals are granted appropriate system access to perform their duties.
II) Minimizing the risk of the data or systems being compromised.
III) Authorized individuals properly access and utilize the data and systems.
IV) Authorized individuals properly maintain confidentiality of all data and systems.

The System Administrator is accountable for instating, maintaining and communicating the various procedures to ensure the continuous control over access security in the LDARD. Such procedures should be specific that all the domain and departmental systems users are held responsible for their own user IDS and passwords.

4. Purpose and objectives

The purpose of this document is to establish the rules and standards for the domain and departmental systems users in the Limpopo Department of Agriculture and Rural Development.

The following are the main objectives of this policy:

i) To ensure that access to information resources is controlled and based on business requirements.

ii) To ensure the implementation of appropriate user access control measures so as to manage the risk of breach of confidentiality, integrity and system availability.

5. Authority

This policy is issued under the custodianship of the Accounting Officer and the Honourable MEC for Agriculture and Rural Development in Limpopo.

6. Legal Framework

- SITA Act, of 1998
- Public Service Act, No 103 of 1994
- Electronic Communication and Transaction Act. Act 25 of 2002.
- Departmental Information Security Policy

7. Scope of application

This policy applies to employees, contractors, consultants, temporaries, and other workers at LDARD including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by LDARD such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

8. Definitions

Authentication	establishing the validity of a claimed entity/verification of the identity of an individual or application

9. Policy Pronouncements

9.1 SITA STANDARD

Security standards regarding a user's COMPLETE ID is provided by SITA (Security Server Standards Documents), www.sita.co.za.

These standards stipulate inter alia:

1) That an ID will be assigned to a user and may under no circumstances be shared.
2) The same applies to the associated password.
3) Users are fully responsible for protecting and save keeping their own ID and password.
4) Users are fully responsible that they do not leave their work station unattended when still logged on the domain and departmental systems.
5) Users are responsible to log off at all times when parting from their workstation.
6) Users should at all times ensure that their station is free of suspicious devices.
7) Users must ensure that their computers are off when they go home.

9.2 GRANTING OF USER ACCESS

User access to information resources are authorised as a result of a formal verification procedure. The procedure should contain the following:

a) User access permissions to pertinent systems shall be authorised.
b) A user access request form shall be completed to grant logical access rights.
c) Effective communication between HR, user department and IT shall be in place to ensure that logical access is granted when responsibilities change or when hiring a new employee.
d) Authentication of users shall be checked prior to user access granted to information resources.

Users are allocated with a username and password. For government employees engaged directly on a permanent basis by the department the username is their PerSal number and they are given a temporary password which must then be changed by them. Temporarily engaged employees, and third party contracted users (including consultants) their usernames will be their surname and initial (i.e. Name Surname will be assigned surnamen@domain.org.cntry or domain\surnamen).

9.3 MAINTAINING USER ACCESS RIGHTS

The review of user access right is necessary to maintain effective control over access to data and information service.

9.3.1 Servers user access

Every quarter, the IT Manager must do a System Admin Access Audit. He/she must validate that the user that have administrative rights to all systems are still relevant. The report will be reviewed quarterly and amended accordingly. The procurement database will also be monitored.

Also after any changes such as:

i) Promotion.

ii) Demotion.

iii) Termination of employment.

iv) When moving from one section /division to another within the same organization.

9.3.2 Standard user access

System administrator must pull out a monthly report of inactive users on the Domain controller for more than 2 months. These users must be blocked / deactivated. The report will include the user name and the reason for being inactive. A decision will be taken whether to temporarily deactivate or remove the user permanently. The report will be reviewed monthly in the GITS team meeting. The report will be kept for audit purposes.

User access right shall also be reviewed after any changes such as:

a) Promotion

b) Demotion

c) Termination of employment

d) When moving from one section /division to another within the same organization

9.4 MINIMUM PASSWORD REQUIREMENTS

1) A password must have a minimum of 8 characters in length (Longer is generally better).

2) A password must contain at least one alphabetic and one numeric character.

3) A password must be significantly different from the previous passwords.

4) A password cannot be the same as the logon username.

5) A password should not be information easily obtainable about the user. This includes license plate, identity number, telephone numbers, or children's names, etc.

6) A password must contain both upper and lower case characters (e.g., a-z, A-Z).

9.5 ADMINISTRATOR/ROOT PASSWORD

a) Powerful accounts such as the Administrator or Root accounts should be set to a highly complex password.

b) The password shall be sealed in an envelope and stored securely in a safe the Administrator password shall be used in emergencies such as system restoration during disaster recovery scenarios.

c) Only authorized personnel are able to retrieve the password and must be logged for record keeping purposes.

d) The password shall be changed immediately after usage, resealed in an envelope and securely.

9.6 PASSWORD MANAGEMENT

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

1) Keep password confidential.
2) Avoid keeping a record of password, e.g. hard copy of electronic file.
3) Change password whenever there is any indication of possible system or password compromise.
4) Compromise passwords that are:
    a) Easy to remember.
    b) Of sufficient minimum length, e.g. six characters.
    c) Not based on anything or somebody else could easily guess or obtain using person – related information, e.g. Names, telephone numbers, date of birth, etc.
    d) Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionary).
    e) Free of consecutive, identical, all –numeric or all –alphabetic characters.

5) Change password at regular intervals or based on the number of times access has been obtained. The password for privilege account should, however, be changed more frequently than normal password.

6) Avoid the reuse or cycling of old password.

7) Change temporary password at first logon.

8) Never share individual user password among users.

9.6.1 Password Reset System

A password management system (Microsoft Forefront Identity Manager – FIM) is in place to aid in the user password management.

1. One chooses a choice of five (5) security questions from a list of available questions and provides the answers to the questions.
2. When one forgets their password, they will need to access the password reset system through a web interface and provide their username.
3. The system will put the user through the security challenge where one answers three of their initially selected five (5) security questions.
4. Upon successful answering of the security questions the user will be allowed to change their password.

9.7 AUDIT TRAILS

The system shall maintain an audit trail of events related to access control. Audit logs shall be retained for an agreed period of time so that investigation of specific incidents can be pursued. Without appropriate audit records it is difficult to hold users accountable for their actions.

The following reports must be used to control and maintain access to the systems.

a) Domain controller security log weekly report.

b) Departmental Systems Access Audit quarterly report.

c) System Admin Access Audit quarterly report.

d) Password resetting weekly report.

e) Inactive users' monthly report.

9.8 FREQUENCY CHANGE OF PASSWORD

i) The Administrator Account user name must be changed every 12 month. The Administrator Account password must be changed every 30 days or if there is any indication that the account has been compromised. The new password should be written on a piece of paper and sealed in an envelope that is stored in a safe.

ii) All new Standard users will have to change their passwords on their first log on to the network.

iii) Should the user not comply with the guidelines, then access to the network or the computer system will be denied.

9.9 PASSWORD RESETTING

Users shall be positively identified, unique passwords shall be issued and secure delivery and immediate forcing of the changing of the issued password shall form the basis in the method of issuing resetting of password.

9.10 USER ACCESS ACTIVITY MONITORING

A) Monitoring of the user activities on the domain and departmental systems:

A set of controls should be defined for controlling and monitoring user access to and activities on the system. The following activities will be done to monitor user activity:

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

b) Any block or suspended user ID (three or more consecutive failed attempts) should be investigated that the user is the authorized owner of user ID and not a 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 60 days should be blocked.

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

e) The department should be prepared to react appropriately should a breach of access such as an unauthorized intrusion be detected.

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

B) Monitoring of the action of the system administrator:

i) The Director: GITO will perform random checks whether the Domain and departmental systems administrator handles all aspect according to this Policy regarding adherence to procedure manual on the user account management.

ii) They will also verify whether all documentation were completed and correctly filed for easy reference

iii) National Treasury has the right to review and monitor the actions of the BAS system controllers.

9.11 ROLES AND RESPONSIBILITIES

A) System Administrator's responsibilities

1) The system Controller is ultimately responsible for access security in the Department.
2) He/She is responsible for creating creation, maintaining and termination of user Accounts.
3) He/She is responsible for joining users to the domain at the Head Office. The District Network Administrators are responsible for creating and joining users at the districts and municipalities.
4) He/She is also responsible for monitoring security logs to see any suspicious activities and further investigate and resolve.
5) He/She is responsible for Password resetting.
6) He/She is responsible for User audit checking users that are inactive.
7) He/She is responsible for keeping records of all documents required for audit purposes.

B) User's responsibilities

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

User should be advised to, inter alia:

a) Terminate active sessions when finished, unless such session can be secured by an appropriate locking mechanism, e, g. a password protective screen saver.

b) Log computer off at end of session (i. e .it not sufficient to just switch off PC screen or terminal).

c) Secure computer from unauthorized use by means of a key lock or an equivalent control, e.g. password access, when not in use.

10 Default

No deviation from this policy is allowed. Should any deviation be needed, it will only be granted with the written approval of the Accounting Officer – after thorough investigation and motivation.

1) Any attempts to bypass security controls or to obtain unauthorised access or to make unauthorised use of a user account belonging to someone else shall be considered a security violation.
2) The use of LDARD's information assets for purpose other than for authorised business purposes shall be considered a security violation.
3) The use of LDARD information assets for any unauthorised or illegal activity shall be considered a security violation.
4) Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure shall be considered a security violation.
5) Any act (or failure to act) that results in sensitive or business critical information being disclosed to an unauthorised person shall be considered a security violation.
6) Any act (or failure to act) that results in sensitive or business critical information being modified or destroyed such that the LDARD or any of its branches / sub branches is adversely impacted shall be considered a security violation.
7) Any breach of this policy or any of its related documents shall be considered a security violation.
8) Any person charged with a security violation shall face disciplinary action.
9) All information abuses and security breaches should be reported to the Information Security Officer.

11 Inception date

The date of approval (as indicated on the cover page of this policy) is also the date of inception.

12 Termination and review

This policy should be reviewed every 24 months (2 years) or as and when a need arise.

13 Enquiries

All enquiries regarding this policy should be directed towards:

The Director: IT

Limpopo Department of Agriculture and Rural Development

PO Box 9487

POLOKWANE

0700

Tel: 015 294 3000

E-mail: ITHelpDesk@agric.limpopo.gov.za

Recommended by:

M Mabuschagne ..... 03/06/2016 .....

Maisela, RJ **Date**

(Head of Department)

Approved by:

..... 03/06/2016

Matshoge, BAJ **Date**

(MEC for Agriculture and Rural Development)