LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
COOPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

PASSWORD POLICY

Revised Date: 22 September 2011

Version: Final

Version Control

Version	Date	Author(s)	Details
Draft 1.0	06/06/2007	Leonard Langa	Draft Password Policy
Draft 1.1	12/06/2007	Leonard Langa	Consolidated inputs from GITO
1.2	27/05/2008	Leonard Langa	Adoption by Labour Management Forum
Draft 1.0	06/06/2007	Leonard Langa	Draft Password Policy
Final	22/09/2011	Leon Nieuwoudt	Departmental Name change update

Contents

1. Preamble

Passwords are one of the primary mechanisms that protect potentially sensitive official information systems and other resources from unauthorised use. While passwords are not the most secured way of protecting information and information systems, constructing secure passwords and ensuring proper password management is essential. Poor password management and protection can allow both the dissemination of information to undesirable parties and unauthorised access to COGHSTA resources. Poorly chosen passwords can be easily compromised. Password compromise can lead to inappropriate disclosure and use of COGHSTA resources or sensitive information and also disclosure of personal information. Training users in the proper password creation and management greatly reduces these risks.

2. Terms and definitions

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action

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

Availability: being accessible and useable upon demand by an authorised entity

Confidentiality: the principle that information is not made available or disclosed to unauthorised individuals, entities or processes

identification and authentication: functions to establish and verify the validity of the claimed identity of a user

information and communication systems: applications and systems to support the business, utilising information technology as an enabler or tool

information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorised manner

monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information

password: confidential authentication information composed of a string of characters

remote access: the access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection

GITO: Government Information Technology Office(r)

COGHSTA: Department of Co-operative Governance, Human Settlements and Traditional Affairs

VPN: Virtual Private Network

Espionage: Obtaining electronic data while not being authorised for personal gain

Cryptographic devices: Devices to encrypt and decrypt electronic data

3. Purpose

The purpose of this policy is to establish minimum rules, guidelines and standards for passwords creation and management used to logon to COGHSTA information systems.

4. Scope

This policy applies to all user accounts provided by COGHSTA to all COGHSTA employees, contractors and service providers that requires access to COGHSTA information computers, network and systems.

5. Objectives of this policy

The objectives of this policy are to:
Provide standards on how to manage and create passwords in the Department to protect electronic data, information and system access.

6. References

The following publications govern the execution of the Password Policy and were taken into consideration during the drafting of the guidelines and policy:
State Information Technology Act (Act no 88 of 1998).
Protection of Information Act (Act no 84 of 1982).
Minimum Information Security Standards (MISS), Second Edition March 1998

Departmental Internet Usage Policy,
Departmental Email Policy,
Departmental Password Policy,
Departmental ICT Equipment Usage Policy.

7. Policy Statement

All user accounts used to logon to COGHSTA information systems shall be protected with strong passwords. Furthermore, passwords must be changed regularly to avoid unauthorised access to information and information systems. Passwords that are not managed properly are at risk of accidental disclosure overtime.

8. Requirements

8.1 Every user shall have a unique username. For COGHSTA employees this shall be the user's Persal number and the date of birth for service providers, contractors and temporary staff. This date of birth shall be in the format DDMMYYYY.

8.2 User accounts for temporary staff, contractors and service providers shall be set to automatically expire on the last day of the contract. Should the contract be renewed, the user shall be required to re-apply for network access. GITO shall only re-enable the user account after receiving the new user application.

8.3 Initial passwords shall be uniquely created by a random password generator and shall be communicated to the user in a secure manner. The user shall automatically be forced by the computer system to change this initial password upon initial user logon.

8.4 Passwords shall not be blank.

8.5 A password history of 20 passwords shall automatically be stored by the authentication system and as a result users must not use previously used passwords when changing passwords.

8.6 User passwords shall be changed every 42 days.

8.7 Default system administrator accounts shall be renamed and their passwords revealed on a need-to-know basis to authorised personnel only.

8.8 No passwords shall be stored in clear text or reversible encryption.

8.9 The system administrator in charge of user management shall only give initial passwords, unlock accounts or reset passwords once the password reset request form is completed and the identity of the user has been validated.

8.10 The least privilege principle shall apply when creating new user accounts.

8.11 If a user's password has expired or the user has forgotten the password, then the user must complete a "Request for Reset of Password Form (Appendix A) and send it to ICT Helpdesk for processing. This is to ensure that all requests to reset passwords are recorded for auditing purposes and to prevent unauthorised resetting of other individual's passwords. GITO may at its discretion require the user requesting the request to physically present him/herself.

8.12 Passwords used within COGHSTA shall not be used for external internet accounts and service providers.

8.13 Passwords shall not be included in any automatic login process.

8.14 New passwords shall not bear any relation to old passwords e.g. password1 and password2.

8.15 Passwords shall contain a mixture of special characters, alpha-numeric characters in lower and upper cases e.g. P@s$w0Rd can be used instead of password.

8.16 Pass phrases shall be used instead of highly complex passwords to prevent the need to write the password where it can be accessed by unauthorised individuals, e.g. Take Cover can be converted to T@k3_Cov3r.

8.17 Passwords from dictionaries in any language are easily guessable and shall be avoided.

8.18 Passwords shall not be identical to the user ID, names, surname, computer name, job title or anything that an attacker can guess.

8.19 Passwords shall have a minimum of 8 characters

8.20 Passwords shall consist of a mix of special and alpha-numeric characters

8.21 Passwords shall not be the same as the username, first name, surname, street address or any words contained in a dictionary of any language

9. Password Protection Guidelines

9.1 Never write usernames and passwords on keyboards, walls, monitors, post-it notes, tables or any material. A memorised password is not prone to accidental disclosure.

9.2 Your password is secure and shall not be shared with anyone including but not limited to colleagues, managers and GITO personnel. This exempts generic departmental passwords i.e. passwords used and managed by a group in a specific department.

9.3 Any file that stores passwords shall be encrypted or password protected.

9.4 New passwords shall not be a simple change of the old password e.g. adding a number at the end.

9.5 Passwords or pass phrases shall not be sent via email or communicated verbally except in cases of password resets and initial user creation between a GITO personnel and the user involved.

9.6 Passwords shall be changed immediately upon disclosure or suspected disclosure.

9.7 Passwords shall not be written or saved in electronic documents unless these documents are encrypted and the user ensures that the encryption keys cannot be accessed by unauthorised individuals.

9.8 Computers shall be locked when the user moves away from the computer to prevent unauthorised access.

10. Account and Password Protection

A user account shall be locked out for a minimum of 24 hours after three failed attempts in order to protect accounts and passwords from brute force attacks or password guessing. Upon account lockout, only the system administrator can unlock the account at the request of the user involved.

11. System-Based Password Requirements

Privileged and administrative passwords shall be subject to stringent composition and frequency of change. Privilege passwords include passwords for routers, switches, firewalls, IPSes, network operating systems and any other IS resource.

12. Best Practices for System-Based and Server Passwords

12.1 All Passwords shall be documented in the password book and kept in the safe at all times. Only authorised personnel shall access the safe. The combination/code for opening the safe shall be divided into three unique codes, one for each authorised individual who must be available to open the safe

12.2 Default factory passwords shall be changed immediately after installation

12.3 Accounts created for external contractors shall be given restrictive rights to carry out their functions and the accounts shall be disabled immediately following the completion of the appointed task

12.4 Privileged passwords shall not be communicated via telephone, fax, email or any printed form

12.5 Administrator/privilege passwords shall not be disclosed to external contractors

12.6 A number of shared local administrative passwords shall be used on machines for specific divisions and computer networks

12.7 The SNMP community strings shall be changed from the standards defaults and shall be different from the password used to interactively log in

12.8 Critical systems shall implement account lockout policies and be set up to disconnect idle sessions after a period of inactivity of thirty minutes

12.9 All servers must be configured not to display the last logon username

12.10 Passwords shall be at least eight characters long but preferably longer

12.11 All systems shall wherever possible be set up to prompt the user to change passwords in 30 days

12.12 Service accounts shall not rely on admin accounts/passwords

12.13 The root/super user password shall never be used unencrypted across the network to avoid eavesdropping. Wherever possible you must **su** to root using SSH or similar technology or use sudo

12.14 Passwords shall be unique from all previous passwords. The last twenty passwords must not be re-used

13. System Administrators

System administrators and those that have system administrator roles shall configure COGHSTA information systems to comply with this Password Policy. System administrators and information security personnel should work with users in an effort to ensure that they are able to comply with this policy.

14. Application/Web Developers

Application and Web developers developing applications that require password authentication shall create code that complies with this Password Policy.

15. GITO

GITO shall provide training, develop, enforce and review this policy, and participate in policy exceptions review. The General Manager of GITO shall participate in policy exceptions review and serve as the final arbitrators in policy exceptions review.

16. Exceptions for Non-Compliant Systems and/or Users

Individuals that are unable to comply with the COGHSTA Password Policy shall request an exemption from GITO. GITO will process the request for final approval via the policy exceptions review. If after review, there is still disagreement over a decision, it may be appealed to the General Manager GITO. The decision of the General Manager GITO will be final.

17. Consequences for Non-Compliance

Any person or entity found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment, termination of any access to COGHSTA network. Violation of this policy may also lead to termination of contracts and commitments to vendors and other entities.

18. Implementation

This policy comes into effect from the date of approval.

19. Policy review

This policy shall be reviewed annually.

COMPILED BY

-- ------------ 28/09/2011

SENIOR MANAGER: Acting **DATE**

INFORMATION TECHNOLOGY

ACKNOWLEDGED BY:

The departmental Password policy has been revised to reflect AG's comments and departmental name change.

28-09-2011

GENERAL MANAGER: **DATE**

GOVERNMENT INFORMATION TECHNOLOGY OFFICE

ACKNOWLEDGED BY:

Noted and supported for approval

24/10/2011

SENIOR GENERAL MANAGER: **DATE**

SHARED SERVICES

ADOPTED /~~NOT ADOPTED~~:

02/11/11

HEAD OF DEPARTMENT **DATE**

APPROVED/NOT APPROVED

approved

09/11/2011

HONOURABLE MEC **DATE**

LIMPOPO PROVINCIAL GOVERNMENT REPUBLIC OF SOUTH AFRICA DEPARTMENT OF COOPERATIVE GOVERNANCE, HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS	**INFORMATION TECHNOLOGY**	Logged By:	
		Call No:	
		015-294-2490	

REQUEST TO RESET USER PASSWORD

Person Details: Person who wants the User Account Password Reset

Surname:		Persal No:	
Full Names:			
Branch:		ID Number:	
SBU:			
Division:		Job Title:	
Telephone No:	( )	Cellular No:	
Office Number:		Floor No:	
Building:		Town:	

Request Details

Date of Request:	
Reason for Password Reset:	
Outline any Information Resources Possibly Compromised:	

Signatures

Approval	*Name*	*Signature*	*Date*
User:			
Manager: Division			
Implemented by (Network Controller:			
Verified by (IT- Deputy Manager:			
Approved by (GITO – Manager):			

ATTACH PRINT-OUT FROM PERSAL SYSTEM SUPPORTING "CONFIRMATION OF APPOINTMENT"

SUBMIT COMPLETED FORM TO ICT CALL CENTRE, 28 MARKET STREET, 2ND FLOOR

LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
COOPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

INFORMATION TECHNOLOGY

Logged By:	
Call No:	

015-294-2490

REQUEST FOR NEW USER ACCOUNT / UPDATE ACCOUNT DETAILS

Person Details: Person who wants the User Account

Surname:		Persal No:	
Full Names:			
Current Username:		ID Number:	
Branch:			
SBU:			
Division:		Job Title:	

Do you need Email Y □ □ Do you need Internet Y □ □

Telephone No:	( )	Cellular No:	
Office Number:		Floor No:	
Building:		Town:	

Divisional Manager

Full Name:		Telephone No:	( )
Surname:		Cellular No:	

Workstation Details

Computer Make:		Computer Model:	
Barcode Number:		Serial No:	

Application Type

New Application [ ] Update Details [ ] Re-Application [ ]

Reason:	

Acceptance of Departmental Policies : Initial next to each to confirm acceptance

Policy Name	*Initial*
ICT Security Policy	
Email Use Policy	
Internet Acceptable Use Policy	
Password Policy	

Signatures

Approval	*Name*	*Signature*	*Date*
User			
Manager: Division			
Implemented by (Network Controller):			
Verified by (IT – Deputy Manager):			
Approved by (GITO-Manager):			

ATTACH PRINT-OUT FROM PERSAL SYSTEM SUPPORTING "CONFIRMATION OF APPOINTMENT"

SUBMIT COMPLETED FORM TO ICT CALL CENTRE, 28 MARKET STREET, 2ND FLOOR