LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
CO-OPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

ICT USER ACCOUNT MANAGEMENT POLICY

Date: 20/02/2012

Version: 1

Version Control

Version	Date	Author(s)	Details
Draft 10	25/08/2011	Thando Mubva, Richard Selepe and Mamakoa Isaac	Draft ICT User Account Management Policy
Draft 11	22/11/2011	Thando Mubva	Alignment to Good practice guide from AG
Draft 11	20/02/2012	Thando Mubva	Circulation to all staff members
Final	27/02/2012		Adopted by Labour Management Forum

Contents

1. Preamble

ICT user accounts are one of the primary mechanisms that protect potentially sensitive departmental network and information resources from unauthorized use. While accounts administration and monitoring are not the most secured way of protecting information and information systems, constructing secure ICT user accounts and ensuring proper password management is essential. Poor ICT user account management and protection can allow both the dissemination of information to undesirable parties and unauthorized access to departmental network resources.

2. Terms and definitions

Account Holder / User: Any person granted an ICT user account with the Department

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

CoGHSTA: Department of Corporate Governance, Human Settlements and Traditional Affairs

GITO: Government Information Technology Office(r)

ICT network user account: An authorised user account, provided to a user, to be used solely by that user, for the purpose of accessing services as granted to that user account

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

ISO: Information Security Officer

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 ICT 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

User: Any person using any of the Department's Information Technology Facilities

VPN: Virtual Private Network

3. Purpose

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to CoGHSTA. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This policy establishes standards for issuing accounts, creating password values, and managing accounts.

4. Scope

This policy is applicable to those responsible for the management of ICT network user accounts or accessing shared information or network devices. This policy covers departmental accounts as well as those managed centrally. The policy further applies to all officials, service providers and other stakeholders.

5. Legal Framework

5.1 ISO 17799

5.2 Information Security Forum (Code of good practice for Information Security)

5.3 Minimum Information Security Standards

5.4 Limpopo Information Security Policy

5.5 Protection of Information Act

5.6 International Standard for Risk Assessment

5.7 COBIT Framework

5.8 Departmental ICT Password Management Policy

6. Policy Content

All user accounts used to logon to COGHSTA ICT network and information resources 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. See approved Departmental policy on Password management.

7. User Registration Management

Accounts that access departmental ICT network and information resources require prudent oversight. The following security precautions should be part of account management:

71 User Registration

7.1.1 The line managers of Coghsta shall make decisions regarding access to their respective data (e.g., the Registrar will determine who has access to registration data, and what kind of access each user has). Account setup and modification shall require the signature of the requestor's supervisor.
The "Request for user account form" on the intranet web site can be adapted to a department's or offices specific needs to capture necessary requestor and access information.

7.1.2 The identity of users shall be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access (eg, user accounts used for email do not require an identity validation process as thorough as for those user accounts that can be used to modify department budgets).

7.1.3 Passwords for new accounts shall NOT be emailed to remote users UNLESS the email is encrypted.

7.1.4 The date when the account was issued shall be recorded in an audit log.

7.1.5 All managers of accounts (ie GITO officials) with privileged access to all departmental user accounts shall sign a Confidentiality Agreement that is kept in the department file under the care of a Human Resource representative or liaison.

7.1.6 When establishing accounts, standard security principles of "least required access" to perform a function shall always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will do.

7.2 Modification/Changes

7.2.1 The identity of users shall be authenticated before providing them with User account and password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.

7.2.2 A "Request of reset password form" that can be accessible on the intranet website shall be used for password reset. Attach the HR Persal function 431 print-out for proof of identification.

7.2.3 Whenever possible, passkeys shall be used to authenticate a user when resetting a password or activating a guest account, and should comply with the above standards. Passkeys provide one-time access to a system or application and require the user to change to a password of their choice upon initial login. Where passkeys are not feasible, pre-expired passwords shall be used.

7.3 User De-registration

7.3.1 GITO shall issue a unique ICT user account to each individual authorised to access the departmental network and information resources. GITO is also responsible for the prompt deactivation of accounts when necessary, ie, accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

8. Review of User Access

8.1 All accounts shall be reviewed at least annually by GITO official to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. The ISO may also conduct periodic reviews for any system connected to the CoGHSTA network.

8.2 All guest accounts (for those who are not official users of the CoGHSTA) with access to CoGHSTA network resources shall contain an expiration date of one year or the work

completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorised member of the administrative entity managing the resource.

9. Privilege Management

9.1 For access to sensitive information managed by a department, account management shall comply with the standards outlined above. In addition; naming conventions must not cause contention with centrally managed email addresses or usernames. Should the potential for contention arise, the applicable system(s) shall not be connected to the campus network until a mutually satisfactory arrangement is reached.

9.2 Use of shared accounts shall not be allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (eg, management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with ISO.

9.3 Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

10. User Responsibilities

The cooperation of authorised users is essential for effective security. Users should be made aware of their responsibilities for making effective access controls particularly regarding the use of passwords and the security user equipment.

11. Password Usage

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

- Keep passwords confidential.
- Avoid keeping a record of passwords, eg 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.
- 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.

12. User password management

12.1 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 shall never be stored on computer systems in an unprotected form.

- Default vendor passwords shall be replaced as soon as the installation of systems or software has been completed and use designated local administrator password.
- Where technically or administratively feasible, shared ID authentication shall not be permitted.
- Where authentication shall occur external to an application, ie, applications should NOT implement their own authentication mechanism. Instead, external authentication services shall be relied upon, provided by the host operating system, the web server, or the servlet container. [In general, applications programmers are not necessarily familiar with the techniques associated with security protocols, and may inadvertently create security holes. Security services available from these external environments are much more likely to provide a high level of security.
- Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.

13. Monitoring of access user activities

13.1 Those responsible for access to systems/applications/servers, etc protected by high-level super-passwords (or the equivalent) shall have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the super-password holder becomes unavailable.

13.2 These documented procedures, which shall be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the "chain of command" becomes responsible for access to and/or reset of the password.

13.3 Activities done by the default account user (ie Guest, administrator, owner and root) should be monitored on a daily basis.

13.4 All account logs shall be monitored weekly and administrator must sign log reports.

13.5 After three failed attempts of login a user account will be disabled and the user has to follow the process of password reset. Failed attempts shall be logged unless the log information includes password information.

13.6 All inactive accounts for 3 months shall be disabled and it will be activated after a user follows the user account modification/changes.

13.7 All accounts that are inactive for 7 months shall be deleted from the systems.

13.8 Accounts shall be monitored and reviewed.

13.9 Password change events shall be recorded in an audit log and signed off by Manager ICT Security.

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

Individuals that are unable to comply with the COGHSTA ICT Account Management Policy must 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.

15. Administration of the policy

GITO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

16. Consequences of Non-Compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.

17. Policy Review

This policy shall be reviewed annually.

18. Effective Date

This policy comes into effect from the date of approval.

COMPILED BY

16/03/2012

SENIOR MANAGER: **DATE**

INFORMATION TECHNOLOGY

ACKNOWLEDGED BY:

Adoption and approval of ICT User Account Management policy is recommended.

06/03/2012.

GENERAL MANAGER: **DATE**

GOVERNMENT INFORMATION TECHNOLOGY OFFICE

ACKNOWLEDGED BY:

Supported for approval.

08/03/2012

SENIOR GENERAL MANAGER: **DATE**

SHARED SERVICES

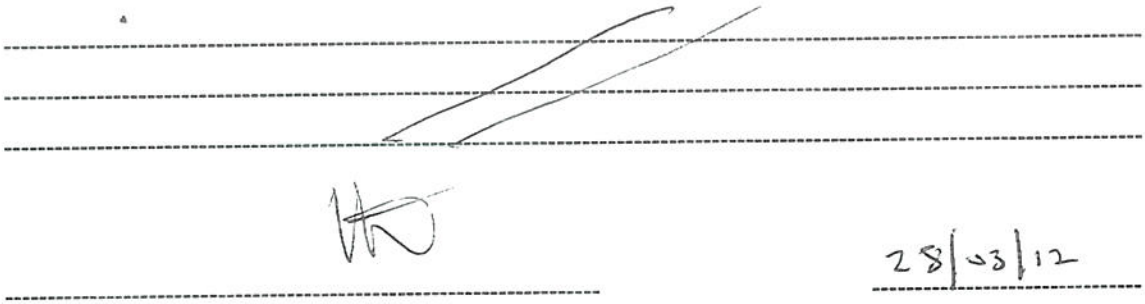
ADOPTED /NOT ADOPTED:

Supported for approval.

08/03/2012.

HEAD OF DEPARTMENT **DATE**

APPROVED/NOT APPROVED



28/03/12

HONOURABLE MEC **DATE**