DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

INFORMATION COMMUNICATION AND TECHNOLOGY USER ACCOUNT MANAGEMENT POLICY

ICTUAMP VERSION 1.0

Document Details

Author	Directorate Strategic Support Services
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Information and Communication Technology User Account Management Policy
Sensitivity	Internal Use Only
Effective Date	After the HoD 's signature
Created Date	28-08-2017
Version Date	<date of HoD signature>

Change Record

Modified Date	Author	Version	Description of Changes

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer & Director Strategic Support Services		30/01/19
Ms S. Mpolokeng	Governance Champion		5/02/19
Ms M.G. Mothibedi	Departmental Chief Risk Officer		08/02/2019
Mr P. Namate	Director Legal Services		11/2/2019

Records Management Sign–Off

Name	Position	Signature	Date
Ms P. Ramokala	Acting Records Manager		13/02/2019

TABLE OF CONTENTS

Glossary of Terms

Audit Log	Is a document that records an event in an Information Technology (IT) system which includes user login details, time, date the account was created.
Critical Information	Information is designated as critical information if its unavailability would have a catastrophic adverse impact on the following: • Client or user life, safety, or health. • Payment to suppliers or users. • Revenue collection. • Communications. • Legal or regulatory.
Data Security	Refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption
DCS&TM	Department of Community Safety and Transport Management
Department	Department of Community Safety and Transport Management
DITO	Department Information Technology Officer
External Stakeholders	Road Traffic Management Corporation (RTMC), Provincial Internal Audit (PIA), Auditor General South Africa (AGSA), Provincial IT, etc.
HoD	Head of Department
Information Communication Technology (ICT)	The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
ICT Systems	For the purpose of this document, ICT Systems means all

	departmental IT Applications.
Information Systems	A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.
ISO	International Organization for Standardization
Logical Access	user based authenticated access to application systems and the data that is processed
MISS	Minimum Information Security Standard
Monitoring	Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.
MPSS	Minimum Physical Security Standard
NWPG	North West Provincial Government
Sensitive Information	Data that must be protected from unauthorized access to safeguard the privacy or security of the department.
Server	A software program, or the specialised computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network.
System Administrator / Controller	An employee designated in the department to manage and control the general functioning of the system
The principle of least privilege	The idea that at any user, program, or process should have only the bare minimum privileges necessary to perform its function. For example, a user account created for pulling records from a database does not need admin rights, while a programmer whose main function is updating lines of legacy code does not need access to financial records.
User	Employee accessing the system for the purpose of processing

	or authorising transaction, updating or amending system data or extracting Management reports from such system

1. Introduction

This Policy is designed to protect the Department, Users and stakeholders from harm caused by the misuse of departmental ICT Systems and data thereof. Misuse includes both deliberate and unintentional actions.

The repercussions of misuse of the departmental systems could be detrimental, if care is not taken. Potential cause and damage includes, but not limited to, Malware infection (e.g. computer viruses), Data leakage which may lead to legal and financial penalties, and Network downtime which may negatively affect productivity.

All departmental users are responsible for the security of ICT Systems and the data thereof. As such, all users must ensure adherence to the guidelines in this policy at all times. In the event of any clarity relating to this policy, the affected user(s) are encouraged to contact the departmental ICT office.

2. Regulatory and Guidance Framework

i. Public Service Act (Proclamation No 103 of 1994)
ii. Protection of Information Act 84 of 1982
iii. Promotion of Access to Information Act 2 of 2000
iv. Protection of Personal Information Act of 2013
v. Electronic Communication and Transaction Act 25 of 2000
vi. Regulation of interception of communication and provision of communication-related information Act 70 of 2002
vii. Public Finance Management Act 1 of 1999 (as amended by Act 29 of 1999)
viii. State Information Technology Agency Act 88 of 1998 (as amended by Act 38 of 2002)
ix. Minimum Information Security Standard
x. Minimum Physical Security Standard
xi. National Cyber Security Policy Framework 2012
xii. ISO 17799
xiii. ISO 27000 series
xiv. ISO 38500
xv. Constitution of the Republic of South Africa (no. 106 of 1996)
xvi. Electronic Communications and Transactions Act (no. 25 of 2002)
xvii. Communication –related information Act (Act no. 70 of 2002)
xviii. Public Service Regulation of 2016, Chapter 6, Section 96
xix. Copyright Amended Act 9 of 2002, Chapter 1, Section 11B

3. Scope of application

This policy applies to all Users of ICT Systems in the Department. However, the policy acknowledges the existence of policies of any other ICT system(s). In cases where a particular system has a policy, such a policy shall therefore take precedence on issues/ areas of contention.

This policy is ONLY applicable to users of departmental specific ICT Systems.

The respective systems supervisors have the responsibility to ensure compliance with this policy document.

4. Use of ICT Systems

All data stored on the departmental systems remains property of the Department of Community Safety and Transport Management.

Departmental ICT Systems exist to support and enable the business of the Department.

A Departmental ICT System administrator shall monitor the use of Departmental ICT Systems and the data on it at ALL the time. This may include, subject to prevailing prescripts, examination of the content stored within the data files of any user, and examination of the access history of any user of the departmental system.

5. Data and Information Security

Departmental data is considered sensitive and confidential; therefore all system users or any other authorised user(s) must treat it as such. Users are therefore expected to exercise caution when disseminating / disclosing information from the Departmental systems to prevent unauthorized access to Departmental information.

Where Departmental data is kept on a portable device, the responsible users must not send, upload, delete or transfer such data that is designated as confidential and sensitive to a non-departmental ICT system.

Users who are supplied with computing equipment(s) must ensure safeguarding of such equipment(s) and data stored in it.

Information on portable devices, such as laptops and tablets, is vulnerable; therefore special care should be exercised with these devices: sensitive information should be stored in protected folder(s) only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not exercised reasonable precautions to secure it.

All ICT equipments (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the responsibility to manage departmental systems are responsible for ensuring that they are at all times properly protected against known and unknown threats and vulnerabilities as far as reasonably practicable and compatible with the designated purpose of those systems.

6. User Registration

- Program Managers (Chief Directors) shall make decisions regarding access to their respective data (e.g. the Chief Director will determine who has access to departmental data, and what kind of access each user has).
- Account setup and modification shall require the signature of the requestor's supervisor.
- 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.
- The date when the account was issued shall be recorded in an audit log.
- 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.
- System Administator/ Controller shall issue a unique user account to each individual authorised to access the departmental systems.

7. User De-Activation

System Administrator/Controller is responsible for the deactivation of accounts when necessary, i.e., 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. User Account Review

- All user accounts shall be reviewed at least annually by System Administrator / Controller to ensure that access and account privileges are in line with their job function, need-to-know, and employment status.
- System Administrator/ Controller shall ensure that all contract workers accounts (officials not employed permanently by the Department of Community Safety and Transport Management) with access to departmental systems shall contain an expiration date of one year or the work completion date, whichever occurs first.
- Access to Departmental Systems by contractors or third parties shall be governed as stipulated in bullet 5.5 of the approved ICT Security Policy.

9. Monitoring User Activities

- There shall be a documented process, which shall be appropriately secured, that should define how 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.
- Activities done by the user (i.e. Guest, administrator) shall be monitored on a daily basis.
- All account logs shall be monitored Monthly and System Administrator / Controller must sign log reports.
- After three (3) failed attempts of login a user account will be locked out and the user has to follow the process of password reset by completing the form

that will be signed by the user and the approval must be granted by the responsible programme manager.

- All inactive accounts for three (3) months shall be disabled and it will be activated after a user has completed the ICT Logical Access Authorization form or any form used for specific systems to reset UserId or Password.
- All accounts that are inactive for six (6) months shall be deleted/ temporarily disabled from the system. (*Care must be taken to archive such accounts activities before deletion*)
- Password change events shall be recorded in an audit log and signed off by the System Administrator.

10. Incident Management

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms) being imported into departmental ICT Systems by whatever means and must where possible report any actual or suspected malware infection immediately to the departmental ICT component. Loss of ICT equipment must be reported to the South African Police Services and Loss Control Committee.

All security incidents must be logged and analysed by the security administration function to identify trends, new risks or gaps in ICT systems. All logged security incidents will remain open until signed-off by the ICT Security Officer, who must be satisfied that all cost-effective countermeasures have been employed to prevent a recurrence of the incident. A summary of all security incidents will be reviewed at the ICT Systems Forum meetings.

11. Unacceptable Use

For the purpose of this policy, "unacceptable use" hereto refers to a usage of the departmental ICT resources i.e. Application of Computing system that is improper or undesirable e.g. carelessness, illegal activities and abuse. The activities below are provided as examples of unacceptable use; however the list is not exhaustive. Should a user wish to contravene these guidelines in order to perform their role(s), they should consult with the departmental ICT

administrator and obtain approval from both their manager(s) and ICT management at senior level before proceeding.

- ❖ All illegal activities. These include theft, computer hacking, malware distribution, usage of illegal or unlicensed software(s) or services. These also include activities that contravene data protection regulations.
- ❖ All activities detrimental to the departmental business goals and objectives. These include sharing sensitive information outside the Department, such as research and development information and customer lists, as well as defamation of the Departmental corporate image.
- All activities for personal benefit/gain that has a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing video and games).
- All activities that are inappropriate for Department to be associated with and/or are detrimental to the Department's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- Avoiding and/or ignoring the IT security systems and protocols which the department has put in place.

12. Password Management

12.1 Password Construction

- Password should be eight (8) to twelve characters in length for more strength;
- Passwords must not consist of repeated character strings (eg. Odu1111);
- Passwords must not consist of sequential numbers or characters (e.g 123456);
- Passwords must be alphanumeric;
- Users must be discouraged from using default passwords;
- Passwords must not mirror the corresponding user id;
- Password must be changed frequently, at least every thirty (30) days.

12.2 Password rules

- Passwords must be kept a secret;
- Do not write down your password, particularly anywhere near your computer or file it in a box file with the word "password" written on it;
- Do not tell or give out your passwords to other people, even for a very good reason;
- Do not display your password on the monitor;
- Do not send your password via email;
- Avoid using the "remember my password" feature associated with some websites, and disable this feature in your browser software. Always click on "Don't remember my password"
- Do not store your password on any media unless it is protected from unauthorised access (e.g. encrypted with an approved encryption method);
- When the user discover that his/her password has been used to access the system, the incident must be treated as a security violation and should be reported to Strategic Support Services immediately;
- Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up.
- The account logout duration shall be 1440 minutes before the user can access the system after reset by the system administrator (*The number of minutes that the locked out account remains locked out before automatically becoming unlocked*)

12.3 Password Administration

- Old passwords must not be displayed at the time of typing the new password;
- System Administrator must be able to revoke passwords;
- Default passwords must have an enforced change on first use (temporary password has to be changed on the first log on);
- User account shall be locked-out after three (3) invalid access attempts;
- ICT Logical Authorization Access Form "Annexure D" shall be completed by the affected user and authorisation shall be granted by the Accounting Officer for the System Administrator to reset password and / or UserId;
- Re-use of at least the twelve (12) previous passwords must not be allowed.

13 User Profiles

- System Administrator / Controller shall maintain a file for each system user and must file any documentation supporting any changes to a user's profile in the User's file.
- System Administrator / Controller shall ensure that all users listed on the system are supported by User Access Forms, at regular intervals (at least on a quarterly basis). Discrepancies shall be monitored closely.

14 Designation of System Administrator(s)

The Program Manager (Chief Director(s)) or his/her delegate shall designate a System Administrator for each of the system used by the department.

A System Administrator:

- shall be responsible for the effective, efficient, economical and transparent use of the system under his/her control;
- Must inform all users about any significant changes that affect the system functionality and/ or operations;
- Shall maintain the system in use through the creation of new codes or removal of redundant codes with the approval of the regulating authority (Accounting Officer);
- Shall monitor if data transactions are of an acceptable standard;
- Ensure safe keeping system reports;
- shall be responsible to compilation and maintaining of manuals regarding the utilisation of the system;
- shall be responsible for identification of problems during the usage of the system;
- shall be responsible for identification of training needs in respect of the system;
- shall serve on Departmental system Forum;
- shall be responsible for controlling of systems in use at regional offices;
- shall be responsible for creation of the new users in terms of the ICT Security policy;
- shall print and distribute relevant reports to other sections that are available on the system;

- shall draw and submit management related reports that are required by the management from time to time;
- Shall regurlaly communicate with users of the system (system users);
- Shall maintain regular backups
- Conduct any other system related duties that may develop from time to time;

15 Enforcement

The Department will not tolerate any misuse of ICT systems and will discipline anyone found to have contravened this policy, including not exercising reasonable judgment regarding acceptable use. Use of any Departmental ICT resources for any illegal activity shall be dealt with in terms of the disciplinary procedures. While each situation will be judged on a case-by-case basis, users should be aware that to a large extend, consequence management will apply.

16 Resolution

This stage focuses on post-investigation activities which include:

Disciplinary Actions

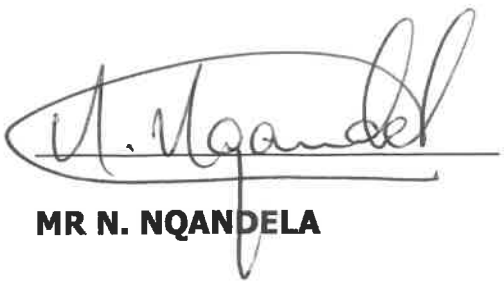
The disciplinary actions will be the results of the findings from the internal investigations. System users who are found to be in breach of ICT User Account Management Policy will have their system access revoked.

17 Review

This policy shall be reviewed every three (3) years and/or when the need arises.

18 Approval

This policy is approved by the Accounting Officer and is applicable with effect from the date of approval below.



MR N. NQANDELA

ADMINISTRATOR

31/01/19

DATE

dcs&tm

Department:
Community Safety & Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

ICT LOGICAL ACCESS AUTHORIZATION FORM

ANNEXURE D

Applicant's Personal Details	
First Name	
Surname	
ID No.	
Email	
Phone Number	
Fax Number	
Company / Department	
Section	
Location	
User ID/Persal No	

Please Tick where applicable:

New User ID		Reset User ID		Reset Password		Request for Reports		Remove System Access	
Specify Application:			Specify Application:			Specify reports:		Specify Location:	

If not listed above, kindly describe your request in detail, e.g. Access to specific server and folder:

Please sign below:

Applicant:

Signature: _____ Date: _____

Duly Authorised by Accounting Officer/delegated:

Initials: ____ Surname: _____

Tel: _____

Signature: _____ Date: _____

Department Stamp

"Together We Move North West Forward"