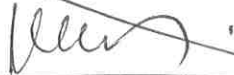


WEST RAND DISTRICT MUNICIPALITY



COMPUTER ACCOUNT MANAGEMENT PROCEDURE

<u>NAME AND POSITION</u>	<u>DATE</u>	<u>SIGNATURE</u>
Wz Kolozi MUNICIPAL MANAGER	10/12/2024	

CONTENTS

1.	COMPUTER ACCOUNT MANAGEMENT PROCEDURE.....	1
1.1	Definitions.....	1
1.2	Purpose	1
1.3	Scope.....	1
1.4.	Roles and responsibilities.....	1
2.	PROCEDURE	2
2.1	Account Administration Standards.....	2
2.2	Identification and password complexity.....	3
2.3	Issuing Accounts	5
2.4	Username.....	5
2.5	Account Status	6
2.6	Account Holder Entitlements.....	6
2.7	User Account Management – Access Reviews	6
2.8	Departmental Accounts	7
2.9	Shared Accounts	7
3.	ADMINISTRATION OF PASSWORD CHANGES	7
3.1	Procedures For Password Resets.....	7
3.2	Procedures For Maintenance Of "Shared Secrets"	7
3.3	Server Administrator Passwords.....	7
3.4	Desktop Administrator Passwords.....	8
3.5	Guest ID.....	9
3.6	Storage And Transmission	9
3.7	Password User Responsibilities	9
4.	Application and system standards.....	10

1. COMPUTER ACCOUNT MANAGEMENT PROCEDURE

1.1 DEFINITIONS

The definitions are described in the table below

TERM	DEFINITION
WRDM	Shall mean West Rand District Municipality
ICT	Shall mean Information and communication
ED	Shall mean Executive Director
HR	Shall mean Human Resources
MM	Shall mean Municipal Manager

1.2 PURPOSE

The purpose of this Procedure is to establish a standard for the administration of Computer accounts that facilitate access or changes to WRDM data. 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 Procedure establishes standards for issuing accounts, creating password values, and managing accounts.

Passwords are the most frequently utilized form of authentication for accessing a Computer resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Password use must therefore adhere to the Procedure statement found below

1.3 SCOPE

This Procedure is applicable to those responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application or shared file space. This Procedure covers departmental accounts as well as those managed centrally.

This Procedure applies to anyone accessing or utilizing the WRDM's network or data. This use may include, but is not limited to, the following: personal computers, laptops, WRDM-issued cell phones, and hand-held factor Computer devices (e.g., PDAs, USB memory keys, electronic organizers), as well as WRDM electronic services, systems and servers. This Procedure covers departmental resources as well as resources managed centrally.

1.4. ROLES AND RESPONSIBILITIES

1.4.1 ICT Manager

To ensure that only authorized personnel are domain admins.

To ensure that only authorized personnel can make changes on user accounts.

To ensure all new accounts are created following procedure.

To ensure consolidation of terminated accounts.

To ensure access review is performed regularly on information systems.

To liaise with HR regarding staff onboarding and terminations to ensure timely termination from information systems.

1.4.2 Administrators / Network controllers / Network Administrator / Server administrator

To remove dormant user accounts

To create users.

To disable offending accounts for security.

To ensure group policy is enforced.

To ensure user and computers are in the correct organizational unit.

1.4.3 ICT Technicians

To ensure users are authenticated on to the network.

To ensure endpoint devices are joined to the WRDM domain.

To ensure endpoint devices utilize AD authenticated account on all machines.

To ensure users do not have admin access to end point devices.

To ensure TCP/IP settings are up to standard on all end point devices.

1.4.4 ICT Steering committee

To ensure timely review of the ICT policies and procedures

To advise on amendments and implementation of the policies and procedures

To recommend reviewed ICT policies to serve at other committees of council prior to approval

1.4.5 Internal audit

To assess business processes within ICT

To assess the efficacy of risk management efforts

To evaluate internal controls and provide improvement recommendations

To assess governance risk and compliance within ICT.

2. PROCEDURE

2.1 ACCOUNT ADMINISTRATION STANDARDS

Accounts that access electronic Computer and information resources require prudent oversight.

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes.

A password is a unique alphanumeric string only known to the user. A password is traditionally associated with a user ID to identify and then authenticate a user.

2.2 IDENTIFICATION AND PASSWORD COMPLEXITY

Identification is the method used to distinguish one user from all others. Identification techniques provide a means of providing authorised entry to the WRDM's resources such as workstations, networks and applications. Identification is closely linked to authentication.

Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure. All staff through a consistent practice of sound security procedures, should ensure that their computing equipment is secured at all times.

All passwords must meet the following minimum standards, except where technically infeasible:

- be at least minimum of six alphanumeric characters long.
- contain digits or punctuation characters as well as letters (e.g., 0-9,
- -'!@#\$() _ -' { . }) NOTE: The following special characters cannot be used in passwords for most WRDM systems: *+,1:;<=>?[\] ^ & .
- contain both upper and lower case characters (e.g., a-z, A-Z).
- not be a word in any dictionary, language, slang, dialect, jargon, etc.
- not be solely based on easily guessed personal information, names of family members, pets, etc.
- Not to contain the user's account name or parts of the user's full name that exceed two consecutive characters
-
- Contain characters from three of the following four categories:
 1. English uppercase characters (A through Z)
 2. English lowercase characters (a through z)
 3. Base 10 digits (0 through 9)
 4. Non-alphabetic characters (for example, !, \$, #, %)
- Complexity requirements are enforced when passwords are changed or created.

Parameter settings

- The Minimum password length has been set between 6 and maximum 8.
- Minimum password age in days is set at 30
- Password history size is set at 12
- Password complexity has been enabled and explained as follows:
- Reversible password encryption is enabled
- Lockout duration is set at 30 minutes
- Reset lockout counter in minutes is set at 30 minutes
- Lockout of local administrator account has been disabled

Audit Policy Settings as required by the Auditor-General:

- The following system security auditing features were activated as follows:
- Audit Account Logon Events
- Audit Account Management
- Audit Directory Service Access (Munsoft to apply)
- Audit Policy Change
- Audit System Events

All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured. NOTE: Do not use the password storage feature offered on Windows or other operating systems. This feature creates a password file that is vulnerable to hackers. Passwords should not be inserted into email messages or other forms of electronic communication.

The same password should not be used for access needs external to the WRDM (e.g., online banking, benefits, etc.).

It is recommended that passwords be changed at least every 30 day's. Individual passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent and must have a primary responsible contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.

If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the ICT Department.

Password cracking or guessing may be performed on a periodic or random basis by ICT or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

2.3 ISSUING ACCOUNTS

Departments 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 and Executive Director on the Computer Access Request Form, account modifications will require an authorisation / confirmation email from the supervisor or Executive Director.

ICT shall issue a unique account to each individual authorized to access that networked Computer and information resource. It is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any Computer 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.

When establishing accounts, standard security principles of "least required access" to perform a function must 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.

The identity of users must 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 (e.g., 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).

Passwords for new accounts should NOT be emailed to remote users UNLESS the email is encrypted. (See the specifications for password under 3.1)

2.4 USERNAME

All WRDM user accounts are uniquely identified by a username, where the username may relate to name of the account owner. The format of the username is dependent on the type of account.

A username is issued to an individual for the duration of that individual's affiliation with the WRDM.

In the case of a legal name change where extraordinary circumstances justify a username change, an account holder may be issued a new account, given an application made in writing to HR the forwarded to ICT for consistency.

2.5 ACCOUNT STATUS

The status of a user account may be:

- a. active - an active account is a fully operational account;
- b. expired - an expired account is one where the account password has expired and is required to be reset before the account can be used;
- c. closed (deactivated) - a closed (deactivated) account is one where access to the account is revoked given that the account holder no longer satisfies the criteria for holding that type of WRDM account (Note the WRDM retains closed accounts for a defined period after which time they are deleted. Until deleted the account can be reinstated to the account holder); or
- d. withdrawn (restricted) - a withdrawn (restricted) account is one where the users' access to the account is withdrawn in advance of the official closure of the account. Refer under each account type for further details on withdrawing access to an account.

2.6 ACCOUNT HOLDER ENTITLEMENTS

The WRDM provides an extensive range of Computer and networking facilities to user account holders, including email, internet access, calendar, modem access, and access to other systems integrated with the WRDM's account system. Access to these services is based on the privileges of the account's type and any individual system's access assigned to the individual account holder.

2.7 USER ACCOUNT MANAGEMENT – ACCESS REVIEWS

Access to systems shall be reviewed regularly by ICT to ensure that access and account privileges are in line with job function, need- to-know, and employment status. The ICT department may also conduct periodic reviews for any system connected to the WRDM network. The account access review will be monitored quarterly.

All guest accounts (for those who are not official members of the WRDM community) with access to WRDM Computer 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 authorized member of the administrative entity managing the resource.

2.8 DEPARTMENTAL ACCOUNTS

For access to sensitive information managed by a department, account management should 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 WRDM network until a mutually satisfactory arrangement is reached.

2.9 SHARED ACCOUNTS

Use of shared accounts is not 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 (e.g., management of file shares).

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

3. ADMINISTRATION OF PASSWORD CHANGES

3.1 PROCEDURES FOR PASSWORD RESETS

Whenever possible, helpdesk should be used to log a ticket 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, these could also be used. Where passkeys are not feasible, pre-expired passwords should be used.

Automated password resets are available and may be utilized, provided that a recognized and approved method is used, such as multiple, random challenge and response questions.

3.2 PROCEDURES FOR MAINTENANCE OF "SHARED SECRETS"

Those responsible for access to systems/applications/servers, etc. protected by high-level super-passwords (or the equivalent) must 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.

3.3 SERVER ADMINISTRATOR PASSWORDS

In addition to the general password standards listed above, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

Passwords for servers must be changed as personnel changes occur.

If an account or password is suspected to have been compromised, the passwords must be changed immediately.

Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks.

Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported.

NOTE: Log files should never contain password information.

3.4 DESKTOP ADMINISTRATOR PASSWORDS

In addition to the general password guidelines listed above, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Network Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported.

3.5 GUEST ID

A guest ID is associated with an account that does not have a specific, individual user ID but rather a more generic ID such as may be required when a contractor is to be given access.

Such accounts are generally intended for temporary use by an authorised visitor and must;

- be kept to a minimum
- have an owner responsible for their management and to ensure passwords are reset for each user
- have access limited to a list of application programs only and have, at most, restricted network access

3.6 STORAGE AND TRANSMISSION

PIN and passwords are automatically classified as CONFIDENTIAL and must be protected appropriately.

If passwords or PINs are stored on hosts, they will be encrypted. Under no circumstances are PIN and password information to be stored in clear text on hosts, even if they do not relate to the host on which they are stored.

Clear text PIN or passwords must never be embedded into application or user files, end user device emulator or file transfer set-ups, etc unless on a computer stored or operated in a proven secure area.

PIN or password files must be stored separately from the main application system data

3.7 PASSWORD USER RESPONSIBILITIES

Users must follow good practice when managing their user IDs, PINs or passwords. Good end user practices in the selection and use of PIN and passwords are essential.

All users are required to adopt the following practises when setting and managing their PIN and passwords:

- Select PINs and passwords that conform to the WRDM's minimum standard. Don't use a weak password just because it's easier to remember.
- Only reveal your user ID if requested by an authorised person; e.g. system administrators or helpdesk personnel trying to resolve a support issue.
- Keep all PIN and passwords confidential;
- Don't give your password to ANYONE. Don't give it to your manager, your spouse, your friend, the VC, your mother, or any other authority!

- Don't write down your user ID or password: remember it. It's better to have your password reset because you forgot it than to have it stolen
- Change PIN and passwords whenever there is any indication of possible system or PIN or password compromise;
- Change PIN or passwords for privileged accounts, e.g. those that access system utilities, every 30 days;
- Change initial PIN or passwords at the first logon;
- Do not include PIN or passwords in any automated logon process, e.g. stored in a macro or function key.
- You are responsible for ANY activity using your account user ID and password.
- Don't let anyone observe you entering your password. Cover your keyboard when logging in if someone is watching you, or ask them to turn away.
- If your password has been changed or reset and you didn't request it or change it, please let ICT know.

The following strategies will help users to generate a password that is easy to remember, is hard to guess and complies with the WRDM's policy.

- Use a mixture of upper and lower case and punctuation e.g. Keep Out!
- String several words or parts of words together e.g. it's Cold
- Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. Tw1nLit* (from twinkle, twinkle, little star), Yat550ml (from you are the sunshine of my love)

Invent phrases like car registration plates e.g. one4you!

4. APPLICATION AND SYSTEM STANDARDS

Applications developed at WRDM or purchased from a vendor should contain the following security precautions:

- 4.1 Where technically or administratively feasible, shared ID authentication should not be permitted.
- 4.2 Authentication should be enforced prior to access to any system.
- 4.3 Passwords must not be stored in clear text or in any easily reversible form.
- 4.4 Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.

Where technically or administratively feasible, systems should allow for lock-outs after a set number of failed attempts. Access should then be locked for a certain time frame, unless a local system administrator intercedes. Lock-outs should be logged unless the log information includes password information.

5. REVIEW

The policy will be reviewed biennial