Molemole Municipality

ICT Policies and Procedures

IT-05-02
User-ID and Password Policy

Document Name: UserID and Password Policy

Date Issued: 31 May 2022

Document Information

Policy	User-ID and Password Policy
Date Issued	31 May 2022
Manual	IT Policies and Procedures Manual
Section	05 Security
Applicability	This applies to all users of the municipal systems and services as well as administrative user accounts.
Situations	This policy is used when users are allocated User-IDs and are provided with user accounts as well as when users create or change passwords and for general security enforcement, when system passwords are changed and allocated, and when it is necessary to change passwords to meet enforced expiry of passwords or for response to suspicion of security threat.
Policy Owner	IT Manager
Policy Enforcer	IT Manager

Contents

1. Overview

1.1. General Purpose

Information and information resources are valuable assets of Molemole Municipality and they form an important part of the operation and management of the municipality.

1.2. Background to this Policy

UserIDs and Passwords are the primary mechanism to provide access control to information services and systems within the municipality and they form an integral part of the total information security function.

Weak passwords and poor application of password policies limit the effectiveness of security policies and electronic access control.

2. Scope

This policy concerns the creation of UserIDs for providing a person with access to a user account, and also with the processes and standards for managing passwords within the municipality.

This includes the creation of suitably strong passwords, the detection and prevention of weak passwords, the frequency of required password changes and related issues concerning governance of passwords in the municipality.

Guidelines are provided as to the creation of suitable passwords.

This is related to all of the security policies within the scope of the ICT Policy Framework. There is specific mention of the Information Sensitivity Policy by this Password Policy.

This policy is not concerned with authorisation available from access to the information resources. Once a user logs on they have access to the resources as provided in terms of other policies, procedures and standards.

3. Purpose of this Policy

The purpose of this policy is to ensure that security is implemented though the effective implementation and management of suitably strong passwords for the restriction of access to information services.

The loss of a system password may severely impact the municipality as a whole and these passwords must be created and managed according to a strict standard of management.

The loss of a user password may impact the municipality in relation to the level of authority and access of the affected user. Such a loss may allow another person to impersonate a user in violation of acceptable use policies and in violation of legislation.

4. Applicability

4.1. This Policy is applicable to the following situations:

- All users of the municipal network, in terms of their access to the information services, systems and equipment which they are authorised to use and to change.
- All system accounts which provide high-level access to systems, servers and equipment at the administrative level.
- The need to change passwords on a regular basis in terms of this policy.
- The need to manage user passwords and system passwords at their appropriate level of classification in terms of the Information Sensitivity Policy.
- The need to respond urgently to security threats and risks arising from loss or disclosure of passwords.

5. Definitions for this Policy

5.1. **Back-door**: this is a way in which security on specific application systems can be bypassed. These are commonly used in the development phases of new applications.

5.2. **Ciphertext**: this is the internal manner in which passwords are stored in secure systems. This prevents access to the actual password as entered by the user, but allows for verification through the usage of mathematical one-way functions (not defined further).

5.3. **Default Password**: this is a password which is provided by default by the developers of systems or by the makers of equipment which is installed.

5.4. **Information Resources**: this includes all information services, systems, databases, equipment, places and devices that are managed in an information security structure. These include Email facilities, Web and

Internet access, workstations, laptops, software on all computers, servers and file systems, secure locations such as server rooms, network equipment including routers, scanners, printers, cabling, data, databases and anything else which is encompassed within the totality of the information services.

5.5. **Information Security**: a functional area within the IT Unit which is responsible for the implementation of all information security policies, procedures, standards and guidelines.

5.6. **Information Security Manager**: the head of the Information Security functional area.

5.7. **Password**: a combination of acceptable characters which when used in conjunction with a user ID provides access to the municipal network and its resources, or to other ICT controlled equipment or systems.

5.8. **Plaintext**: this is the form of the password that is as the user enters it, as opposed to ciphertext, which is how it is stored internally within secure systems.

5.9. **Remote Access User**: any user who gains access to the information services through remote access services such as dial-up or VPN.

5.10. **Single-Sign On (SSO):** an approach to password-based security in which a single user logon provides access to a range of information services, each of which respect the credentials of the user from their original logon to the common network. All application systems must be structured to support network authentication rather than requiring an additional user code and/or password for each application system or network resources. This does not apply to system passwords.

5.11. **Strong Password**: a password which is likely to be immune to password-breaking programs or to be discovered by guessing.

5.12. **System Password**: a password associated with a system or administrative service or equipment or place. These include the administer-level accounts on servers, databases and application systems, the key codes that provide access to secure facilities such as server rooms, and passwords that enable administration access to routers and other network equipment.

5.13. **User**: this includes all users who use the municipal network and its associated services, systems and equipment for access to information services, as well as information on workstations and storage devices.

5.14. **UserID**: the code provided by Information Security which is used to uniquely identify an individual user account or a system account. The UserID is the basis for authentication of a valid user, when used in conjunction with a password, and is also the basis for allocation of authorised access and for all security monitoring concerning users.

5.15. **User Account**: the range of information resources associated with a valid User and may include Email, server access and access to specific information systems and services.

5.16. **User Password**: the password associated with providing access to a User Account.

5.17. **Weak Password**: a password that has the potential of being discovered by electronic means including software designed to break passwords or being discovered by guessing.

5.18. **Workstation**: applies to all computing devices used to access the information resources including desktop computers, terminals, laptop computers, notebook computers, PDAs and mobile phones.

6. References for this Policy

6.1. ECT Act : Electronic Communications and Transactions Act.

This provides certain requirements in terms of the handling of communications and transactions which concern security in general, but is not specific to password requirements.

6.2. IT Compliance Management Guide V1.0 (October 2008), published by Microsoft Corporation).

This provides a useful classification in terms of the management of passwords used for authentication in an information services environment.

6.3. MISS : Minimum Information Security Standard.

This provides the minimum requirements for information security within public sector institutions.

Chapter 7 of the MISS is particularly relevant to this password policy, although the MISS only provides high-level guidance.

6.4. SANS Institute : Password Policy.

Password policies are consistent throughout IT implementations throughout the world and there is virtually no difference between countries whether this is in the public or private sectors.

The SANS Institute Password Policy has been used as the basis for this policy.

7. Policy Statements

7.1. Every person accessing the municipal information resources is required to have their own unique UserID.

7.2. A UserID is provided in terms of the Request for UserID Procedure. This provides the basis for allocation of a user account. A UserID must be created using the standard for UserIDs.

7.3. When it is necessary to update information about a user account, then the Procedure: Update a User Account must be used. It is not permitted to update or change a UserID after this has been allocated to a user.

7.4. No user is allowed to have more than one UserID.

7.5. Every user account is provided with access to information resources as are deemed appropriate to the specific user for carrying out their work. This is beyond the scope of this policy.

7.6. The allocation of a UserID and a corresponding user account does not imply the provision of all information services, such as Internet Access and an Email address.

7.7. When a user is provided with access to Email facilities their Email address must be the same as their logon UserID.

7.8. Internet access is a privilege and not a right of the users. If an existing user requires access to the Internet as part of their job function, then this must be done in terms of the Procedure: Request for Access to Internet Resources.

7.9. When a person is no longer permitted access to information resources their UserID must be cancelled. In such cases the same UserID must never be reused, and all archives associated with the UserID must be retained in terms of the Data, Information and Records Policy (04-01).

7.10. UserIDs must only be disclosed to others who need this information, such as those needing to exchange information by Email. UserIDs must be not disclosed for any other purpose.

7.11. A user is responsible for all activity taking place using their personal UserIDs.

7.12. Users must not use passwords to lock their computer which will deny access to Information Security, such as boot passwords and overriding or using an administrator password. As required, Information Security may manage the administrator-level access to all user workstations.

7.13. All system passwords must be managed in a secure manner using the System Level Password Management Standard.

7.14. All user-level passwords (as are used for network access, Email, web access, desktop computer, screen savers) must be changed at least every month.

7.15. Users who have system passwords must use the system password allocated using the System Password Management Standard to access the information services provided by these system passwords.

7.16. Passwords must not be reproduced in any way or form which may compromise security of the user account or system account. This includes writing passwords and keeping them in “secret” places in the offices, writing passwords into diaries or other personal documents, inserting passwords into email messages, or keeping passwords in the contents of files on electronic storage on networks or workstations.

7.17. All user-level and system-level passwords must conform to the standards and guidelines provided below.

7.18. Passwords must be maintained using the “automated preventive” (IT Compliance Management Guide, p21) method of management where this is possible. This must provide for automated expiry of the passwords by internal server operations and security rules, and the automated compliance with password strength guidelines.

7.19. Where possible, access to municipal systems and services must use an integrated approach to user account and access, as is commonly referred to as Single Sign-On or SSO.

8. Standard: UserIDs

8.1. All UserID are formed by taking the first name of the user and appending the first letter of the surname. For example JOHNS for John Smith.

8.2. UserID are always case-insensitive, so that johns and JOHNS and JohnS all refer to the same user.

8.3. In situations in which this would lead to duplicate names, additional letters must be used from the users name rather than to use digits. It is important to ensure that in this situation user codes are sufficiently distinct to ensure that the right user code can be identified easily.

9. Standard: Logon Authentication

9.1. Every time a user gains access to the information resources, they are required to enter their UserID and Password.

9.2. When a user is entering a password, they must ensure that no-one is in a position to see what they are entering by seeing the keys which they press. It must be noted that it is polite to look away when this information is entered.

9.3. Workstations must never be set up to use the facility of remembering UserID and passwords. It is noted that Microsoft Windows cannot be set up to remember passwords when used with the CTRL-ALT-DEL logon procedure.

9.4. Users will be locked out after three unsuccessful logon attempts.

9.5. After a UserID is locked out, it can only be unlocked by Information Security.

9.6. Workstations must be set up to log off automatically after a maximum of 15 minutes of non-usage.

9.7. Users must lock their workstations using CTRL-ALT-DEL or must log off if they leave their workstation unattended.

10. Guidelines: Creating Strong Passwords

10.1. Passwords are used for various purposes within the municipality. These purposes include providing access to the following types of information services:

- user accounts
- remote user access
- system accounts
- web access
- email accounts
- workstation logon and locking

- screen saver protection
- voicemail password
- routers, switches and other networking equipment
- server access
- database access
- application access for administrators

10.2. Some systems and services already provide for one-time passwords (such as the OTP facilities for on-line banking systems), and for these situations this Guideline does not apply.

10.3. Weak Passwords have the following characteristics:

- They are the original default password associated with the service, equipment, user account or other facility being protected.
- The password contains less than 8 characters (user passwords) or 10 characters (system passwords).
- The password has been used previously for the same purpose or are slight variations of previously used passwords
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Common words associates with the municipality and local places.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.

- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- Any combination of words and letters which is predictable by users knowing a previous password.

10.4. Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~- =\`{}[]:";'<>?,./)
- Are at least 8 alphanumeric characters long (user password) or 10 alphanumeric characters long (system passwords)
- Are not the same as previously used passwords, nor are slight variations of previously used passwords
- Are not words that may be found in a dictionary for language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Are never to be written down or stored on-line.
- Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- NOTE: Do not use either of these examples as passwords!

11. Standard: Password Protection

11.1. Do not use the same password for user accounts as for other information security requirements such as home computers, other online services and web sites.

11.2. Where possible, don't use the same user password for various municipality access needs.

11.3. Never share user passwords with anyone, including administrative assistants or secretaries, family and friends, or other employees. If this has to be done on a temporary basis to provide access to someone else for support purposes, then change the password immediately after the support session has been completed.

11.4. All passwords are to be treated as sensitive and must be treated as CONFIDENTIAL information in terms of the Information Sensitivity Policy.

11.5. The following guidelines apply in all cases:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

11.6. If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

11.7. Do not use the "Remember Password" feature of applications as is available with most web browsers. This will compromise your user account if your computer is stolen.

11.8. Do not write passwords down and store them anywhere in your office.

11.9. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

11.10. Change passwords at least once every month (changes for system passwords are identified in the System Password Management Standard).

11.11. If an account or password is suspected as having been compromised, report the incident to Information Security and change all passwords.

11.12. Password cracking or guessing may be performed on a periodic or random basis by Information Security or its delegates.

11.13. If a password is guessed or cracked during one of these scans, the user will be required to change it.

12. Standard: System Level Password Management

12.1. The Information Security Manager or their delegate is responsible for the management of system passwords and the changing of passwords on the respective systems, access control units and equipment.

12.2. The loss of a password for system level access may severely inhibit the ability of the municipality in the operation of its services, and this may pose a significant risk to the municipality as a whole. At the extreme this may completely disable all functions of the municipality that rely on the information network and systems.

12.3. All system level passwords must be allocated the information sensitivity level of SECRET and managed appropriately in a secure physical environment in accordance with the Information Sensitivity Policy (04-03).

12.4. All system level passwords must be known to at least three people at all times and these people must be available at all times.

12.5. All IT systems, services, physical access points, and equipment which must be secured by system passwords and the complete list of these system passwords and the resources that they secure must be kept in a list called the System Password List.

12.6. The System Password List must identify the system passwords and the level of access to which resources granted by each system password. It must also keep the list of all historical passwords used in order to ensure that no password is used more than once, in cases in which there is no system for automated prevention.

12.7. All system level passwords must be changed at least every 6 months.

12.8. When a person is given a system level password this is maintained in a register called the System Password Allocation Register which is kept with the System Password List. The System Password Allocation Register is updated to indicate which person has been provided with which passwords, at which time, and for what purpose, and whether there is an expiry to this allocation for temporary access requirements.

12.9. If the allocation of the system password is for temporary use, then the system password must be changed immediately after the expiry of the temporary use period.

12.10. When a person is no longer authorised to access the resources being protected by system password, such as when an employee leaves the employment of the municipality or a contract is completed, then all systems passwords they have been allocated must be changed

immediately, and all other persons who use these passwords be notified that these have changed and be requested to obtain the updated passwords.

12.11. Whenever it is suspected that system security has been compromised in any way then all affected system passwords must be changed immediately, and be redistributed to those who need them for their daily work. The permission for this must be obtained from the IS Manager for this situation.

12.12. When system passwords are changed, the changes must not be predictable by a person knowing the previous passwords. In particular the system passwords must not be created using any pattern or formula.

13. Standard: Application Development and Passwords

13.1. Application developers must implement specific security policies within programs designed to run in the municipal environment. The applications must be developed on the basis of the following principles:

- must use security which is integrated with municipal security structures in promoting a single-sign on (SSO) security model if this is available within the municipality and when the technologies support this approach.
- must support authentication of individual users, and not groups, although allocation of rights may be provided at a group level.
- must not store system passwords in plaintext or in any easily reversible form with on data files, databases or in program code.
- must provide “back-door” access only during periods of development and not within live environments.
- must provide for role management, in which authorized access is provided at the level of the role. In this situation one user can take over the functions of another without having to know the other's password.

14. Standard: Use of Passwords and Passphrases for Remote Access Users

14.1. Access to the municipal networks via remote access must be controlled using the same security and user passwords as are used by internal users.

14.2. For situations in which additional security is required, authentication must be based upon one-time passwords public/private key system with a strong passphrase.

15. Procedure: Request for New User Account

Trigger

15.1. This procedure is triggered by a request for New User Account.

Requester

15.2. Any person allowed to request the new user account in terms of this policy.

Responsibility

15.3. The IT Officer will be responsible.

Steps

Seq	Activity	Who	Duration
1	Requestor completes the Form 05-51 : Request for New User Account.	Requester	
2	Requestor hands completed form to IT Officer.	Requester	
3	Admin Officer checks the form, to ensure that all the forms are filled in properly.	Admin Officer	
4	If the form is incomplete, then inform requester to complete the form before applying again.	Requester	
5	The IT Manager provides policies to the requester and ensures that they understand the policies before asking them to sign the form and acceptance of the policies.	IT Officer Requester	
6	IT Officer requests IT Manager to approve by signing.	IT Manager	
7	IT Officer provides form to IT Manager who opens and prepares a new user account for the requestor.	IT Manager	

Forms and Registers

15.4. Form 05-51 : Request for New User Account / Update Details

Practice Notes / Additional Notes

15.5. Must never fast-track the process by side-stepping the explanation of the policies and requesting requester signature.

15.6. Never process applications without all necessary signatures in place.

15.7. For users who require access to the payments processes, including expenditure and salaries, the CFO must also sign the approval.

15.8. For users who require access to the HR systems, the Director Corporate Services must sign.

15.9. In the case of contractors, this must also be signed by the SBU Manager of the Unit in which the contractor is working on a contract.

15.10. By signing the form the user agrees to comply with the Acceptable Use Policy and Internet Use Policy if Internet access is to be provided, as well as Email Use Policy if an Email account is to be created.

15.11. The Form is presented to Information Security who creates the user account and creates the UserID and an initial one-time password which must be changed at the first logon.

15.12. Information Security also provide access to specific information resources as requested on the form, such as email accounts and Internet Access. As required, limits may be placed onto the usage of resources.

15.13. For this and all other procedures in which Forms are presented to Information Security in order to instruct them to carry out specific user account changes, these Forms must be maintained in a suitable register or file for future reference in order to audit this policy.

Enforcement

15.14. This procedure is enforced by the IT Officer and IT Manager.

16. Procedure: Request to Update User Details

Trigger

16.1. This procedure is triggered by the request to update user details

Requester

16.2. Any person requesting update for user details.

Responsibility

16.3. The IT Officer will be responsible.

Steps

Seq	Activity	Who	Duration
1	Requestor completes the Form 05-51: Request for New User Account / Update Details.	Requestor	
2	Requester hands completed form to the IT Officer.	Requestor	
3	IT Manager checks the form, to ensure that all the forms are filled in properly.	IT Manager	
4	If the form is incomplete, then inform requester and hand back the form.	Requester	
5	Present form to IT Manager for approval of changes.	IT Manager	
6	Request that the IT Manager update the necessary details.	IT Manager	

Forms and Registers

16.4. Form 05-51: Request New User Account / Update Details

Practice Notes / Additional Notes

16.5. As for New Account procedure.

Enforcement

16.6. This procedure is enforced by the Admin Officer and IS Security manager.

17. Procedure: Requesting the Removal of a User Account

17.1. This applies in all situations in which a user account is required to be removed including termination of employment of an employee.

17.2. There is no Form for this procedure.

17.3. In urgent cases a user account can be temporarily locked by Information Services on the basis of a sufficiently authenticated telephone call. The nature of sufficient authentication must be defined internally by Information Security and for security purposes the approach used is not recorded in policy statements and may change from time to time. This must be approved by the IT Manager.

17.4. This must be applied as soon as is possible and practical due to the security risks on maintaining access rights for persons who are no longer permitted access.

17.5. If the process will take longer than anticipated, then the password of the user account must be reset while the user account is being suspended.

17.6. All information concerning the user account, including history of usage, email archives and contents of personal network stores must be archived in terms of the Data, Information and Records Policy.

18. Procedure: Password Reset

Trigger

18.1. Procedure for Password Change

Requester

18.2. Any persons requiring a password change which cannot be done using the normal method within Windows. For example, if the user has forgotten their password.

Responsibility

18.3. The Admin Officer and IS Security Manager will be responsible.

Steps

Seq	Activity	Who	Duration
1	Requestor completes the Form 05-52: Request for Password Reset.	Requester	
2	Requester hands completed form to the IT Officer.	Requester	
3	Admin Office checks the form, to ensure that all the forms are filled in properly.	IT Officer	
4	If the form is incomplete, then inform requester and hand back the form.	Requestor	
5	IT Manager changes the password to a one-time logon password which is required to be changed at the next logon.	IT Manager	

Forms and Registers

The forms used for this procedure Form 05-52: Password Change

Practice Notes

Enforcement

This procedure is enforced by the IT Manager.

Practice Notes / Additional Notes

18.4. Any user may change their password at any time using the network user facilities. This does not require permission from Information Security and is encouraged to be performed on a regular basis.

18.5. This is accomplished as follows:

- At any time after they have logged on, they must press CTRL-ALT-DEL
- In Windows 10 and 11 the system window opens up, and the user can select Change Password…
- The new password is entered, ensuring that the right DOMAIN is also selected for the user.
- The new password is entered again, to avoid the problem of spelling mistakes when entering the password, since the password characters cannot be viewed.

19. Procedure: Request for Access to Internet Resources

Trigger

19.1. This procedure is requesting access to Internet Resources which is not provided by default to new user accounts.

19.2. It is not guaranteed that a user will be granted access. They must motivate this in terms of their job responsibilities.

Requester

19.3. Any persons requesting Access to Internet Resources.

Responsibility

19.4. The IT Officer and IT Manager are responsible for this procedure.

Steps

Seq	Activity	Who	Duration
1	Requestor completes the Form 05-53 Request for Internet Access.	Requester	
2	Requestor hands completed form to the Admin Officer.	Requester	
3	IT Officer checks the form, to ensure that all the forms are filled in properly.	IT Officer	
4	If the form is incomplete, then inform requestor and hand back the form.	Requestor	
5	Ensure that the Requester understands the Internet Use Policy and other related policies and that they sign their acceptance of these policies as well as signing the form.	Requester IT Officer	
6	Submit form to IT Manager to sign approval	IT Manager	
7	Submit to IT Manager to implement the Internet Access with any additional limitations as identified by IT Manager.	IT Manager	

Forms and Registers

19.5. Form 05-53 Request for Internet Access

Practice Notes / Additional Notes

19.6. This procedure is used for situations in which a user requires access to the Internet, including Web and other facilities.

19.7. The Form 05-53: Request for Internet Access must be completed by the user and signed by their next level manager and by the IT Manager and by IT Officer.

19.8. This form requires that by signing the form the user agrees to comply with the Acceptable Use Policy and Internet Use Policy.

Enforcement

19.9. This policy is enforced by the IT Officer and IT Manager.

20. Passphrases

20.1. Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

20.2. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

20.3. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

20.4. An example of a good passphrase is

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

20.5. All of the rules above that apply to passwords apply to passphrases.

21. Standard: Retention of User Code Forms

21.1. The Forms identified in the procedures represent the documentary evidence of work performed in terms of this policy.

21.2. In the eventuality of a conflict in terms of actions taken, the documentary evidence will be the only information suitable for ensuring that the right actions have been taken.

21.3. The signed forms must be retained by the Service Desk in a secure environment, such as a locked cupboard, for reference at any time in the future. These records must be stored by user code, and by date, to ensure ease of access to the records.

21.4. After 3 years these must be archived into the registry or other suitable archive services.

22. Implementation

22.1. Where practical and possible, all of the policies and standards mentioned in this Policy Statement must be implemented through Group Policies that are enforced centrally.

23. Enforcement

23.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

24. Forms / Registers

24.1. System Password List

This list is managed by the IT Officer under the supervision of the IS Manager. This is classified as sensitive information at the level of SECRET, and is required to be managed in accordance with the Information Security Policy.

24.2. System Password Allocation Register

Every person who is allocated a system password is listed on a register concerning who has which system password.

This list is also maintained as SECRET and is required to be accessed whenever the user rights change and it is necessary to reset or change many system passwords at the same time.

24.3. Request for New User Account Form / Update Details (05-51)

24.4. Request for Password Reset Form (05-52)

24.5. Request for Internet Access (05-53).

25. Review and Audit

25.1. This policy will be reviewed every 6 months as part of a standard ICT Policy Review process.

25.2. The enforcement of this policy will be audited using the following guidelines:

- Information Security personnel and all users are aware of the contents of this policy and how it affects their usage of the municipal information resources.
- UserIDs are allocated, changed and removed in accordance with this policy, including the maintenance of a suitable filing system for user account requests.
- User accounts have Email and Internet facilities only if these have been approved by a form signed by the relevant manager.

- Password policies on strength implemented using automated prevention at the time of user logon.
- System Password List maintained and up to date.
- All information resources and other resources requiring access via system passwords are identified on the System Password List – no system resources are omitted.
- System Password List and System Password Allocation Register maintained in accordance with the Information Sensitivity Policy.
- At least two persons have been given each system password.
- Other guidelines as may be applicable in specific situations for resources or as may be required by internal or external auditors.

NB: This policy shall be effective upon approval by the municipal council and shall be reviewed after three years from the date of approval or should the need for review arise.

Cllr. M.E Paya
Mayor