Information Communication and Technology (ICT)

USER AND SYSTEM ACCESS POLICY

Matjhabeng Local Municipality

(MLM)

Contents

1. INTRODUCTION

With evolving technology along with increased risks and threats results in ensuring that a comprehensive user and system access controls are in place to mitigate against threats that could severely jeopardize MLM business critical applications and services. Information security user access controls provides a sound platform that ensures that ICT systems, data and infrastructure are continuously protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as restrictions of unauthorized disclosure or incorrect processing of data.

2. OBJECTIVE AND PURPOSE OF THE POLICY

The objective of the policy is to define the user access management control measures for the MLM ICT systems, information and infrastructure where it would apply to both the MLM users and Service Providers. This policy seeks to protect the privacy, security and confidentiality of the MLM information. The main objective of this policy is to provide the MLM with best practice User Access Management controls and procedures to assist in securing the user access management procedure.

The aim of this policy is to ensure that the MLM conforms to standard user access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. SCOPE

The ICT User Access Management Policy has been developed to guide and assist MLM to be aligned recognised best practice User Access Management controls and procedures. The policy applies to everyone in the MLM, including its service providers/vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the MLM. The policy covers the following elements of user access management:

- New user registration;
- Terminated user removal;
- User permission/role change request;

- User access rights assignment for networks, operating systems, databases and applications;
- Reviewing user access permissions; and
- User and administrator activity monitoring.

4. DEFINITION

Access control rules and procedures are required to regulate who can access MLM Information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing MLM information in any format, and on any device.

5. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The ICT Steering committee must review the policy on an annual basis and recommended changes must be approved by Council.

6. DELEGATION OF RESPONSIBILITY

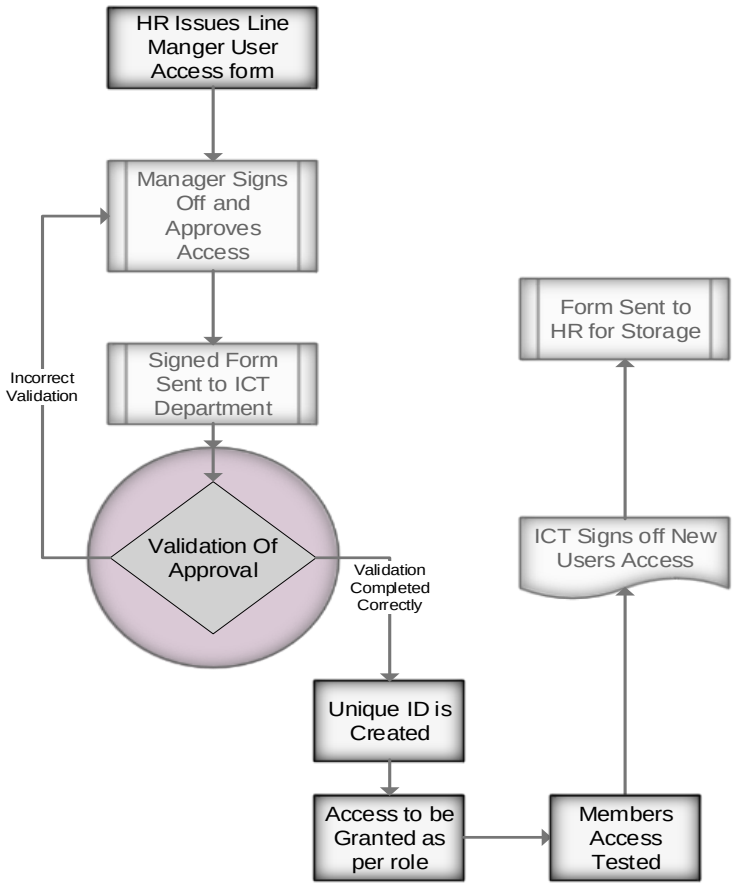
In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

7. NEW USER REGISTRATION

A formalised user registration process must be implemented and followed in order to assign access rights. All user access requests must be formally documented, along with the access requirements, and approved by authorised personnel by making use of the user access request form. The template for this type of request can be found attached to this policy in Annexure A.

- User access requests must be obtained from HR on registration of a new employee.
- The form must be sent to the service provider/line manager for access requirements to be requested.
- Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT department for approval following which the activation of the employee based on the specified requirements will be completed.

- User access must only be granted once approval has been obtained.
- The form must then be sent back to HR for record keeping purposes. Records of user access granted must be stored for a minimum of 10 years.
- All users must be assigned unique user IDs in order to ensure accountability for actions performed. Should shared accounts be required to fulfil a business function, this account must be approved and documented by the Risk Management Committee.
- The diagram below depicts the formal new user registration process to be followed.

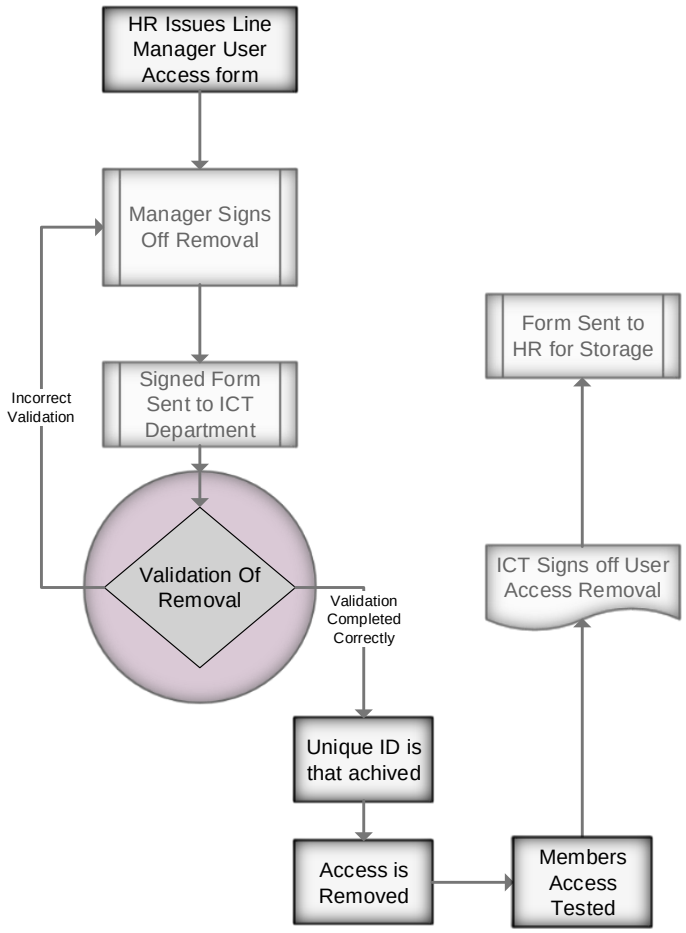


The unique ID must be associated with the HR and easy for members' recognition.
Examples:

Name.Surname
Surname.Name
Surname.Name.EmployeeNum

8. TERMINATED USER REMOVAL

- A formalised user termination process must be implemented and followed in order to revoke access rights.
- All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.
- Terminated user requests must be obtained from HR on the termination of an employee. The template for this type of request can be found attached to this policy in Annexure A. The form must be sent to the service provider/line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access removal must be stored for a minimum of 10 years.
- The diagram below depicts the formal user termination process to be followed:



9. USER PERMISSION/ROLE CHANGE REQUEST

- A formalised user access management process must be implemented and followed in order to adjust user access rights.
- All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.
- Access must only be granted once approval has been obtained by the respective line manager.
- User access change requests must be obtained from HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure A. The form must be sent to the service provider/line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for

record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.

- User access rights that are no longer required must be removed immediately.
- The diagram below depicts the formal user permission/role change request process to be followed. **WHERE IS A DIAGRAM?**

10. GENERAL USER ACCESS RIGHTS ASSIGNMENT

- Access rights include, but are not limited to:
- General office applications (E-mail, Microsoft Office, SharePoint, etc.);
- Department specific applications and/or databases;
- Network Shares;
- Administrative tasks;
- RAS/VPN Access (Remote Access Services and Virtual Private Network)
- Wi-Fi; and
- BYOD (Bring your own devices), this will be fully treated as other Municipality devices.
- Access must follow a “principle of least-privilege” approach, whereby all accesses revoked by default and users are only allowed access based on their specific requirements.
- The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.
- Access rights must be assigned to a group/role. User must then be assigned to that group. Access rights must not be assigned to individual users. **CLARIFY**

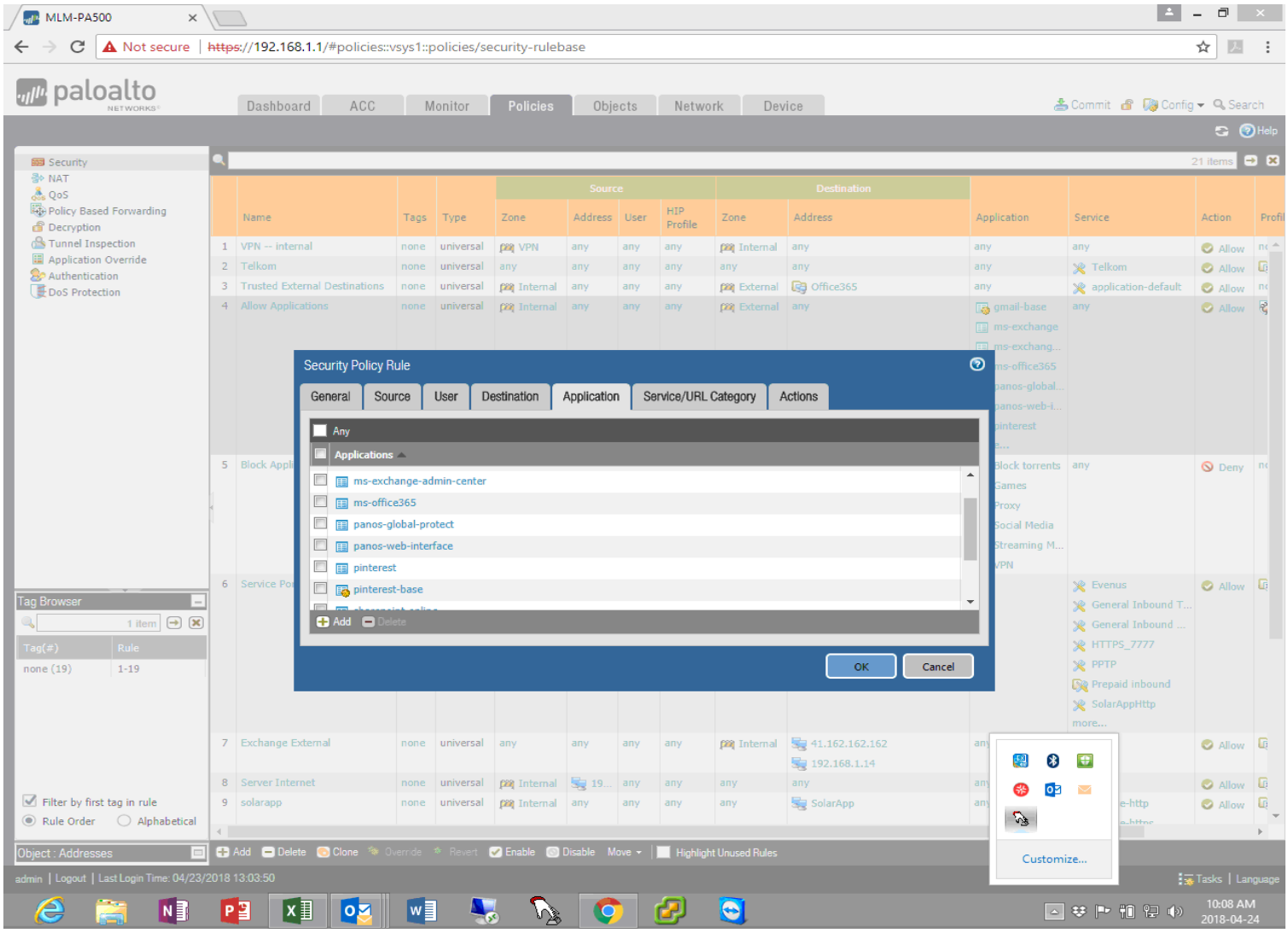
Restricted Access will fall on domains that have been block from accessing specific websites like for example:-

- Social Media Sites (What’s App, Facebook, Instagram etc.
- Streaming Video (Pinterest, You Tube, Supersport, on-line VOD sites)
- Porn
- All restricted sites – This will be based on the firewall SSL sites for intrusion.

Certain IP addresses will conform to the unrestricted usage of the internet but the integrity of the system must still be maintained.

The allowed list must be within the policy of MLM and must be maintained as key security infrastructure as per the policy rules and regulations current adjustment include the blocked list of websites.

The image below illustrates current list of allowed internet based content and/or sites:



11. NETWORK USER ACCESS RIGHTS ASSIGNMENT

- Access to the Municipality's network must only be allowed once a formal user registration process has been followed.

- Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.
- RAS/VPN access must only be granted to users who require the service to fulfil their business function.
- Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.
- Best practice states that VPN access must only be granted to employees who:
  - Work remotely (Not at the office).
  - Work overtime, or not within regular office hours.

- It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.
- RAS/VPN access must be monitored and audit logs reviewed every quarter (3months) by system administrators.
- All reviews must be formally documented and signed off by the ICT Manager.
- Documentation must be kept for record keeping purposes. **Records of**
- RAS/VPN access reviews must be stored for a minimum of 10 years.
- The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is used for official purposes (BYOD).
- The ICT team must ensure that all mobile devices are protected with a PIN.

12. PASSWORDS

Choosing passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A *weak password* is one which is easily discovered, the basic weak passwords are for example:

"Password123, GOD, Children's names, Spouse's-close relationship names"

A *strong password* is a password that are designed to be difficult to determine by the individuals that are not the owner of the set password:

Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

Passwords should be alpha numeric and changed once a month as set by standard best practise. This can be managed and instituted on a server level.

Example: pinray45

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different MLM systems.

Do not use the same password for systems inside and outside of work

Changing Passwords

All user-level passwords must be changed at a maximum of every 30 days as per the security policy of MLM, or whenever a system prompts you to change it. Default passwords must be changed immediately. If you are aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to IT Helpdesk at MLM Users **must not** reuse the same password within 12 password changes

13. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

Each system administrator must be given their own accounts within the administrator group. Should the need arise for shared accounts being required to fulfil a business function, then this account must be approved and documented by the Risk Management Committee. The default guest account must be removed or renamed and disabled.

14. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place. Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

15. DATABASE USER ACCESS RIGHTS ASSIGNMENT

- The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need this access.
- Municipal employees who use applications may not have these rights to the application's databases.
- The ICT Manager must ensure that Municipal employees who access databases directly (e.g. through ODBC) only have read access.
- The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.
- The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

16. REVIEWING USER ACCESS AND PERMISSIONS

- User access and user permissions must be reviewed every quarter (3 months) by system administrators.
- On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, an investigation into the finding must be conducted.

- On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.
- All reviews must be formally documented and signed off by the ICT Manager.
- Documentation must be kept for record keeping purposes. Records of user access review must be stored for a minimum of 10 years.

17. USER RESPONSIBILITIES

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to MLM systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing IT Helpdesk or the ICT manager of any changes to their role and access requirements. Please note attached Annexure A – User Access Change Document

18. USER AND ADMINISTRATOR ACTIVITY MONITORING

- User and administrator activity must be monitored through audit and event logging.
- Once a month, system administrators and application owners must review audit and event logs for suspicious and malicious activities.
- Dormant accounts should be disabled and a request to remove the access should be performed in line with policy. User Permission/Role Change Request.
- All reviews must be formally documented and signed off by the ICT Manager.
- Documentation must be kept for record keeping purposes. Records of user activity monitoring must be stored for a minimum of 10 years.

ANNEXURE A: USER ACCESS MANAGEMENT FORM EXAMPLE

Name: _____ Date: ___/____/____

Designation: _____Requested by: _____

Department:_____

Please Tick What is Required	
PC ☐ *Laptop☐	
Administrative rights	
E-mail	
VPN	
RAS	
Solar – List all required function in **Appendix A**	
Payday HR ☐ Payday Salaries☐	
Cashdrawer	
Own Device setup	
Other: Specify	

New Application	
Change Of Details/Additional Access	
Removal of Access	

_____

The following section **must be completed** if access is being requested for a service provider/vendor/consultant

Period of access: _____

Reason for request:

_____

_____

HR Manager Line Manager ICT Manager System Administrator

Signature: _____ _____ _____ _____

Date: ___/____/____ ___/____/____ ___/____/____ _____/_____/_____

***ATTACH PROOF OF CAR OWNERSHIP**

TERMS AND DEFINITIONS

Abbreviation Definition
BYOD - Bring Your Own Device
HR - Human Resources
ICT - Information and Communication Technology
ID - Identifier
ISO - International Organization for Standardization
ODBC - Open Database Connectivity
PIN - Personal Identification Number
RAS - Remote Access Service
VPN - Virtual Private Network