EMAKHAZENI LOCAL MUNICIPALITY

USERNAMES AND PASSWORDS POLICY

Approval

DOCUMENT:	**USERNAMES AND PASSWORDS**		
Copy Number:	**Master Copy**		
Compiled by:	Niall Carroll	**Reviewed by:**	
Compilation Date:	August 2013	**Review Date:**	
Version:	V 1.03	**Revision:**	
Distribution:	All	**Classification:**	
Document Release Approval		**Document Acceptance**	
Releasing Authority: Deputy Manager: ICT	ICT	**Acceptance Authority:**	Council
Date Released:		**Date Accepted**	
	Signature:		**Signature:**

DOCUMENT CONTROL

0.1 Revision Record

Revision	Date	Change Record	Changed By
1st		Revised ICT Policy Submitted to Council	N Carroll ICT
2nd	March2013	Reviewed and updated	N Carroll ICT
3rd	August2013	Re formatted layout	N Carroll ICT

0.2 Issue Control

This policy is issued by the Corporate Services Department on behalf of Emakhazeni Local Municipality, to whom any change requests or queries should be directed. The review life for this document is 12 months.

0.3 Distribution

CopyNo.	Name	Title	Organisation
Master			
01			
02			

The MASTER for this document is held electronically and only signed copies are valid. An unsigned, printed document is not copy controlled and is to be used for information purposes ONLY, as it will not be automatically updated. It is therefore the responsibility of the reader to ensure that it is a currently valid copy.

Contents

1. USERNAMES AND PASSWORDS

1.1 All users must have a proper username and a password as mentioned elsewhere in this document that will grant them access to the network and network services available on the network. The name must be compiled in accordance with the naming standards that are authorized and agreed to for the network.

1.2 The username must be in accordance with standards used in all other government levels and departments to ensure a standardized network that can be easily managed and supported and that will adhere to policies and procedures from the National Intelligence Agency and relevant intelligence laws applicable to all levels of government and also organizations that are seen as key infrastructure for the government and the country. One example is to use the surname of each person and the initials of the person. The first seven (7) characters of the surname is used and one initial, normally the first. If there is a duplicate username, the second initial is used. If there is, still a duplicate the whole surname is used or parts of the first name, not only the initial, until there is no duplicate username. In some cases it may be that the people have the same names and surnames and seniority can then be used to differentiate or a nickname by which one of the people is known may be used with the normal username make up. Only the initial should then be used to differentiate. Care must be taken that nicknames are not derogatory to a person or humiliate or offend that person but must be accepted by the person. Where possible however this must be avoided. Care should also be taken that the username does not exceed ten (10) characters as it may encounter problems on some systems and could create problems.

1.3 No user may offer his/her username and password to any person, regardless of rank or designation, to access the network or any network resource available on the network. All users should subsequently be limited to have only one (1) connection to the server and all other network services. Only through application and permission given by the Head of the Department responsible for Information Communication Technology may more than one connection be granted to a user. No user may also use another user's user account (username and password) to gain access to the network for any reason. In such cases the user account must be locked and the case be reported to the relevant Head of Department. It may not sound serious but it was found in many other cases before that individuals using another person's user account committed fraud, corruption or sabotage and such cases had widespread repercussions.

Therefore, such measures are employed to prevent such actions rather than to cure the results of such actions.

1.4 No user is allowed to use the Administrator user account to gain access to the network unless the person has been appointed in writing as the network administrator and have completed the relevant courses in this regard. Accessing this account will give access to areas that should not be accessed by users and may lead to misconfigurations that could incapacitate the network and bring about unnecessary downtime on the network. Downtime that is brought about by users through either intended and/or malicious actions may ensure that the users are charged for the support in order to repair such damage. Since this account has access everywhere on the highest levels contravention of this policy should be reported to the Head of the Department responsible for Information Communication Technology and the relevant department whose member contravened the policy.

1.5 Where people leave the employ of the municipality they should be given the chance to remove any private and personal information from the computer and also ensure that data on the server is official data and not personal data. The user account must be locked for a period of thirty (30) days and e-mail received should be forwarded onto the new address provided. This period will also ensure that the relevant data is copied to the personnel that would need it and allow for the reallocation of personnel where applicable. After this time the user account should be removed from the file server and the system synchronized and updated to reflect the relevant changes.

1.6 All users must use a password to access the network and users should be forced to change all passwords every sixty (60) days. This will ensure a better measure of control against illegal outside attacks and provide a more secure environment. Apart from forced changes, no password may be used concurrently and unique passwords must be chosen. Passwords should not be repeated for at least six (6) months or cycles of password changes.

1.7 All inactive user accounts that are found to be inactive for longer than thirty (30) days should be disabled and locked. This means no access will be possible. It will then force the user to request a password change and reactivation of the user account. User accounts that are inactive for longer than 3 months should be deleted from the system. The data contained in a home directory of such a user should then be copied to a location where it is accessible to other users.