KAMIESBERG MUNICIPALITY PASSWORD POLICY

1. Overview

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

2. Purpose

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

3. Scope

This policy applies to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account.

4. Password Protection

1. Never write passwords down.
2. Never send a password through email.
3. Never include a password in a non-encrypted stored document.
4. Never tell anyone your password.
5. Never reveal your password over the telephone.
6. Never hint at the format of your password.
7. Never reveal or hint at your password on a form on the internet.
8. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
9. Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
10. Report any suspicion of your password being broken to your IT computer security office.
11. If anyone asks for your password, refer them to your IT computer security office.
12. Don't use common acronyms as part of your password.
13. Don't use common words or reverse spelling of words in part of your password.
14. Don't use names of people or places as part of your password.
15. Don't use part of your login name in your password.
16. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
17. Be careful about letting someone see you type your password.

5. Password Requirements

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements will be set by the IT security department:

- Minimum Length - 6 characters recommended
- Maximum Length - 12 characters
- Minimum complexity - No dictionary words included. Passwords should use 2 of the following 3 types of characters:
    - Lowercase
    - Uppercase
    - Numbers
- Passwords are case sensitive and the user name or login ID is not case sensitive.
- Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.
- Maximum password age -30 days
- Minimum password age - 2 days
- Store passwords using reversible encryption - This should not be done without special authorization by the IT department since it would reduce the security of the user's password.
- Account lockout threshold - 4 failed login attempts
- Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value as of the date of writing this article is 20 minutes. This means if there are three bad attempts in 20 minutes, the account would be locked.
- Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal of additional help desk calls. Therefore depending on the situation, the account lockout should be between 30 minutes and 2 hours.
- Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. they can press the CTRL-ALT-DEL keys and select "Lock Computer".
- Rules that apply to passwords apply to pass phrases which are used for public/private key authentication

6. Enforcement

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action.

7. Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.