Information Services Department Policy 1.1
Password Use Procedure
Revision: 1.2
September 24, 2008

Purpose:
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the City of Marysville's entire corporate network. As such, all City of Marysville employees (including contractors and vendors with access to City of Marysville systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Policy:

1. Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of Marysville facility, has access to the City of Marysville network, or stores any non-public City of Marysville information.

2. General Password Policy
A. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.
B. User accounts that have system-level privileges granted through group memberships or programs such as "pseudo" must have a unique password from all other accounts held by that user.
C. Passwords must not be inserted into email messages or other forms of electronic communication.
D. All user-level and system-level passwords must conform to the "Strong" password guidelines described below.
E. All system-level password will be changed immediately upon termination of Information Services administration staff.

3. Password Construction Guidelines
Passwords are used for various purposes at the City of Marysville. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Strong passwords have the following characteristics:
- Are at least eight alphanumeric characters long.
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g.:
  - 0-9
  - !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.

Try to create passwords that can be easily remembered. One way to do this is 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 the above examples as passwords!

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- 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.
  - Proper names like "City of Marysville", "Snohomish", "Washington" or any derivation.
  - 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)

4. Password Protection Standards

Do not use the same password for City of Marysville accounts as for other non-City of Marysville access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various City of Marysville access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share City of Marysville passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential City of Marysville information.

- 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

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

The use of another employee's password on any City-owned computer system is prohibited. If you inadvertently find or receive another employee's password you should inform the employee immediately so they can change their password.

Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer). Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every three months.
If an account or password is suspected to have been compromised, report the incident to Information Services and have your password changed.

5. Application and System Development Standards

Application developers must ensure their programs contain the following security precautions. Applications...

A. should support authentication of individual users, not groups.
B. should not store passwords in clear text or in any easily reversible form.
C. should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
D. should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).