CITY OF TOPPENISH

ADMINISTRATIVE POLICY 2014 – 27

SUBJECT: **COMPUTER PASSWORDS**

DATE ISSUED: **AUGUST 5, 2014**

EFFECTIVE DATE: **SEPTEMBER 1, 2014**

APPROVED BY: _____
William C. Murphy, City Manager

PURPOSE:

This policy supersedes all prior policies regarding the creation and use of passwords on City-owned computers. Because computer passwords are an important aspect of computer security and are the front line of protection for user accounts, all City of Toppenish employees are responsible for taking the appropriate steps to select, secure and periodically change their passwords, as outlined below. There are different tiers of computer users among city employees, each potentially presenting a different risk of exposure to unauthorized access to the City's electronic communications systems and information technology. For that reason this policy establishes different security requirements: one for employees who use a computer for email only (Tier #1); one for employees who use a personal computer (Tier #2); and one for employees who use a personal computer for administrative purposes (Tier #3). All employees are reminded that all uses of the City's electronic communications, computer hardware and software, computer networks, internet, and email are subject to the City's Administrative Policy 2014 - 2, entitled "Electronic Communications and Information Technology Policy."

DEFINITIONS:

1. Tier #1 users: All personnel who use a city computer that is shared with other employees and who are permitted to use it for email only.
2. Tier #2 users: All personnel who have been assigned a city-owned personal computer for his/her exclusive use.
3. Tier #3 users: The Information Technology Specialist (ITS) appointed by the City Manager for all departments except the Police Department; the ITS appointed by the City Manager and the Police Chief for the Police Department; and the Finance Director/City Clerk. These users will also have a Tier #2 user account for daily non-administrative use.

RULES FOR CREATING A PASSWORD:

No passwords shall have any of the following characteristics:

- Less than eight characters
- Be a word found in a dictionary (English or foreign)
- Be a username (log in identification needed to open an account) or any part thereof
- Be a word or words of common usage, such as
    1. Names of family members, pets, friends, co-workers, fantasy characters, etc.
    2. Computer terms and names, commands, sites, companies, hardware, software.
    3. The words "City of Toppenish" or any derivation thereof.
    4. Birthdays and other personal information such as addresses and phone numbers.
    5. Word or number patterns, such as abababa, aaabbb, qwerty, xyzzyx, 123321, etc.
    6. Any of the above preceded or followed by a digit.

In addition, passwords created by all users within the respective tiers must be as follows:

1. Tier #1: no less than 8 characters; changed at least every 120 days.
2. Tier #2: no less than 12 characters; changed at least every 90 days.
3. Tier #3: No less than 15 characters; changed at least every 60 days.

TIPS:

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., aZbY)

- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%"&*(L+I--=\' {} []:";'<>?,.I)

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: "TmB I w2R!" or "Tmb I W>r-" or some other variation.

DON'TS:

- Don't reveal a password to any one in any way, including your family members, your supervisor, administrative assistant or secretary. However, you are required to provide your manager with your passwords to enable continuity of business in the event of your absence. This should be done in a sealed envelope, to be opened only in such circumstances. Managers shall not open such envelopes except in those circumstances. You must also provide your passwords to the ITS for use in installing desktop applications and other maintenance. You must keep your manager and ITS informed of the mandated changes in your password in a timely manner.

- Don't use the "Remember Password" feature

- Don't write passwords down and store them anywhere in your office

- Don't store passwords in a file on any computer system without encryption

- Don't use the same password across multiple sites

- Don't recycle a password, no matter how long it's been since you last used it, because the system currently remembers the last 24 passwords.

- Don't use the same password for various City of Toppenish access needs.

- Don't use your City of Toppenish password for your personal computer or your personal accounts.

- Don't use your City of Toppenish password on any computer other than the one you are authorized to use for City business.

POLICY VIOLATIONS:

Any violation of this policy could lead to discipline, up to and including termination.