PAUL J. FETHERSTON
TOWN MANAGER

# TOWN OF NEWINGTON

131 CEDAR STREET
NEWINGTON, CONNECTICUT 06111

## OFFICE OF THE TOWN MANAGER

**Information Technology Policy**
Effective Immediately
February 1, 2005

**SUBJECT : Password Policy**

**PURPOSE :** To establish a standard(s) for creation of strong passwords and/ or pass phrases, the protection of those passwords/pass phrases, and the frequency of change. Passwords and/ or pass phrases are an important aspect of the Town of Newington's (hereinafter "Town") communication networks security. They are the front line of protection for user & system accounts. A poorly chosen password/pass phrase may result in the compromise of the Town's entire communication networks. As such, all Town employees (including contractors and vendors with access to the Town's communication networks) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords/pass phrases.

**APPLICABILITY:** This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password/pin/pass phrase) on any system that resides at any of the Town's facilities, has access to the Town's communication networks, or stores any non-public Town information.

**1.0 General**

**1.1.** All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

**1.2.** All production system-level passwords must be part of the Information Systems and Technology administered global password management database.

**1.3.** All user-level passwords (e.g., email, web, desktop computer, voice mail, etc.) must be changed at least every ninety (90) days. This is the minimum recommended change interval.

**1.4.** User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

**1.5.** Passwords must not be inserted into email messages or other forms of electronic communication.

**1.6.** 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).

**2.0 Guidelines**

All user-level and system-level passwords must conform to the guidelines described below.

**2.1. General Password Construction Guidelines**

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

**2.3. Poor, weak passwords have the following characteristics:**

**2.4.** The password contains less than eight characters

**2.5.** The password is a word found in a dictionary (English or foreign)

**2.6.** The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.

**2.7.** Computer terms and names, commands, sites, companies, hardware, software.

Phone: (860) 665-8510 Fax: (860) 665-8507
townmanager@ci.newington.ct.us
www.ci.newington.ct.us

**2.8.** The words "Town of Newington", "Newington", "NPD", “NFD” or any derivation.
**2.9.** Birthdays and other personal information such as addresses and phone numbers.
**2.10.** Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
**2.11.** Any of the above spelled backwards.
**2.12.** Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

**2.13.** Strong passwords have the following characteristics:
**2.14.** Contain both upper and lower case characters (e.g., a-z, A-Z)
**2.15.** Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
**2.16.** Are at least eight alphanumeric characters long.
**2.17.** Are not words in any language, slang, dialect, jargon, etc.
**2.18.** Are not based on personal information, names of family, etc.
**2.19.** 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 these examples as passwords!

## 3.0 Password Protection Standards

**3.1.** Do not use the same password for Town accounts as for other non-Town access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Town access needs.
**3.2.** Do not share Town passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, “Confidential” Town information.
**3.3.** Do not reveal a password over the phone to ANYONE
**3.4.** Do not reveal a password in an email message
**3.5.** Do not reveal a password to the boss
**3.6.** Do not talk about a password in front of others
**3.7.** Do not hint at the format of a password (e.g., "my family name")
**3.8.** Do not reveal a password on questionnaires or security forms
**3.9.** Do not share a password with family members
**3.10.** Do not reveal a password to co-workers while on vacation
**3.11.** If someone demands a password, refer them to this document or have them call someone in the Information Systems and Technology Department.
**3.12.** Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer). Information Systems and Technology will disable these items via network group policies to enhance and strengthen overall network security.
**3.13.** 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.

## 4.0 Password Change Frequency

**4.1.** Change passwords at least once every ninety (90) days (except system-level passwords which must be changed quarterly).
**4.2.** If an account or password is suspected to have been compromised, change all passwords immediately and the user SHALL report the incident to Information Systems and Technology.

**5.0 Security/Audit checks**

**5.1.** Password cracking or guessing may be performed on a periodic or random basis by the Town's Director of Information Systems and Technology and/ or his/ her duly authorized designee. If a password is guessed or cracked during one of these scans, the user will be required to change it.

**6.0 Use of Passwords and Pass-phrases for Remote Access Users**

**6.1.** Access to the Town's communication networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass-phrase. See the Town's E-Mail Policy regarding the authorized use of Outlook Web Access and the Town's Virtual Private Network (VPN) Policy for additional requirements.

**7.0 Pass-phrases**

**7.1.** Pass-phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass-phrase to "unlock" the private key, the user cannot gain access.

**7.2.** Pass-phrases are not the same as passwords. A pass-phrase is a longer version of a password and is, therefore, more secure. A pass-phrase is typically composed of multiple words. Because of this, a pass-phrase is more secure against "dictionary attacks."

**7.3.** A good pass-phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass-phrase: "T0r1$wvbt = Traffic on (substituted a zero for an "o") route 15 ($ substituted for a "5") was very busy today."

**7.4.** All of the rules above that apply to passwords apply to pass-phrases.

**8.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**9.0 Definitions**

| Terms | Definitions |
|---|---|
| Application Administration Account | Any account that is for the administration of an application (e.g., Oracle database administrator, ISS administrator). |
| ISP | Internet Service Provider (AOL, SBC, Cox, Comcast, etc.) |
| VPN | Virtual Private Network |
| OWA | Outlook Web Access |

_____

Paul J. Fetherston
Town Manager