PASSWORD POLICY

1.0 Overview

Total Securities Limited is into the business of Securities market broking and uses Computer to Computer Link (CTCL) (CTCL & IBT are hereafter referred as "network") to expand its network and facilitate the dealers and clients. 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 the compromise of **Total Securities Limited's** entire corporate network. As such, all **Total Securities Limited** employees (including clients, contractors and vendors with access to **Total Securities Limited** systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 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 for safeguarding access to the **Total Securities Limited's** network.

3.0 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 **Total Securities Limited** facility, has access to the **Total Securities Limited** network, or stores any non-public **Total Securities Limited** information.

4.0 Policy

4.1 General

CTCL/ IBT system's Password

- The Password is masked at the time of entry.
- Changing of password when the user logs in for the first time.
- Automatic disablement of the user on entering erroneous password on three consecutive occasions.
- Automatic expiry of password on expiry of 14 calendar days.
- The password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical.
- The changed password cannot be the same as of the last password
- The Login id of the user and password should not be the same.
- The Password should be of minimum six characters and not more than twelve characters.
- The Password is encrypted at members end so that employees of the member cannot view the same at any point of time.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at **Total Securities Limited.** Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very 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.

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.
    - The words " **Total Securities Limited** ", "sanjose", "sanfran" 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)

Strong passwords have the following characteristics:

- 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, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are 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 these examples as passwords!

B. Password Protection Standards

Do not use the same password for **Total Securities Limited** accounts as for other non **Total Securities Limited** access (e.g., personal ISP account, option trading, benefits,

etc.). Where possible, don't use the same password for various **Total Securities Limited** access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share **Total Securities Limited** passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential **Total Securities Limited** information.

Here is a list of "dont's":

- 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
- IN SHORT DO NOT REVEAL YOUR PASSWORD TO ANY ONE

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

Do not use the "Remember Password" feature of applications (e.g., odin, outlook, messenger).

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 fourteen days (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

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

6.0 Exceptions
There are no exceptions to this policy.