Password Protection Policy

1.0 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

2.0 Background

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 Kelvin TOP-SET Ltd.'s entire corporate network. As such, all Kelvin TOP-SET Ltd employees (including contractors, casuals, temporaries, third parties and vendors with access to Kelvin TOP-SET Ltd systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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 Kelvin TOP-SET Ltd facility, has access to the Kelvin TOP-SET Ltd network, or stores any non-public Kelvin TOP-SET Ltd information.

4.0 Policy

4.1 General

1. All system-level passwords (e.g., Unix / Linux / AIX root, Windows / NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

2. All user-level passwords (e.g., email, web, laptop, desktop or workstation computer, etc.) must be changed at least every 90 days.

3. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

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

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

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Kelvin TOP-SET Ltd. Some of the more common uses include user level accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Poor, weak passwords have the following characteristics:

1. The password contains less than eight characters

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

3. The password is a common usage word such as:

    a. Names of family, pets, friends, colleagues, television characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, and software.
    c. The words "TOP-SET", “Kelvin TOP-SET” or any derivation.
    d. Birthdays and other personal information such as addresses and phone numbers.
    e. Word or number patterns like aaabbb, qwerty, 123321, etc.
    f. Any of the above is spelled backwards.
    g. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

1. Contain both upper- and lower-case characters (e.g., a-z, A-Z)

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

3. Are at least eight alphanumeric characters long.

4. Are not words in any language, slang, dialect, jargon, etc.

5. Are not based on personal information, names of family, etc.

Passwords should never be written down (e.g., on post-it notes) 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 Kelvin TOP-SET Ltd accounts as for other non-Kelvin TOP-SET Ltd access (e.g., personal ISP account, home banking etc.).

Do not share Kelvin TOP-SET Ltd passwords with anyone, including managers, administrative assistants, or secretaries. All passwords are to be treated as sensitive, confidential Kelvin TOP-SET Ltd information.

Here is a list of "don't":

- 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 holiday
- Don’t leave passwords on sticky notes on your desk

If someone demands a password, refer him or her to this document or have him or her refer to the Kelvin TOP-SET Ltd IT Staff.

If an account or password is thought to have been compromised, report the incident to the Kelvin TOP-SET Ltd IT Staff.

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

C. Application Development Standards

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

1. Support authentication of individual users, not groups.

2. Not store passwords in clear text or in any easily reversible form.

3. 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. Use of Passwords and Passphrases for Remote Access Users

Access to the Kelvin TOP-SET Ltd Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong Passphrase.

E. Passphrases

Passphrases 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 Passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A Passphrase is a longer version of a password and is, therefore, more secure. A Passphrase is typically composed of multiple words. Because of this, a Passphrase is more secure against "dictionary attacks."

A good Passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good Passphrase:

"The*?#>*@TrafficOnTheM56Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to Passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
A contractor found to have violated this policy would be liable to their contract to provide a service terminated.

6.0 Definitions

Term	Definitions
Passphrase	Similar to a password but can be made up of any number of characters. A Passphrase is generally thought to be stronger than a password
LDAP	Lightweight Directory Access Protocol (LDAP), is a protocol used to access a directory listing. It is being implemented in Web browsers and e-mail programs to enable lookup queries.
SNMP	Simple Network Management Protocol (SNMP), is the network management protocol used almost exclusively in TCP/IP networks.

7.0 Revision History

Who	Date	Revision Type	Revision Number
Scott Bowden	20/10/2021	Initial draft	V0.1
Scott Bowden	14/03/2022	Updated	V0.2
Scott Bowden	30/01/2024	Annual check/update	V0.3