Telecoms Advisor Ltd

Password Policy

Review History			
Name	Role/Position	Date Reviewed	Signature

Approval History			
Name	Role/Position	Date Approved	Signature

Overview

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 Telecoms Advisor Ltd's entire network. As such, all employees (including contractors and vendors with access to Telecoms Advisor Ltd's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

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.

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 Telecoms Advisor Ltd facilitator has access to the network.

Policy

General

- All systems-level passwords (e.g., root, enable, network administrator, application
- administration accounts, etc.) must be changed at least every 90 days.
- All production system-level passwords must be part of the Information Security administrated global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused.
- Passwords must not be inserted into email messages or other forms of electronic
- communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

Password Construction Requirements:-

- Be a minimum length of eight (8) characters on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the User ID
- Expire within a maximum of 90 calendar days.
- Not be identical to the previous ten (10) passwords.
- Not be transmitted in the clear or plaintext outside the secure location.
- Not be displayed when entered.
- Ensure passwords are only reset for authorized user.

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:
When a user retires, resigns, is reassigned, released, dismissed, etc. Default passwords shall be changed immediately on all equipment.
Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed:-

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- Supervisor or POC should fill out a password deletion form and send it to [the system administrator who will then delete the user's password and delete or suspend the user's
- account.
- A second individual will check to ensure that the password has
- been deleted and user account was deleted or suspended.
- The password deletion form will be filed in a secure filing system.

Password Protection Standards

X Do not use your User ID as your password.
X Do not share passwords with anyone
X All passwords are to be treated as sensitive,
X Do not reveal a password over the phone to anyone
X Do not reveal a password in an mail message

- X Do not talk about a password in front of others
- X Do not hint at the format of a password (e.g., “my family name”)
- X Do not reveal a password on questionnaires or security forms
- X Do not share a password with family members
- X Do not t use the "Remember Password" feature of applications
- X Do not write passwords down and store them anywhere in your office.
- X If an account or password is suspected to have been compromised, report the incident to your line manager and change all passwords.

Penalties

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