Adventz Securities Enterprises Limited

Password Policy

1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. As such, all employees (including contractors and vendors with access to systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2. 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.

3. 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), has access to the *company's* network, or stores any non-public Information.

4.Policy

4.1 General

- All systems-level passwords maybe changed at least every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) may be changed at least every 120 days.
- 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.

4.2 Guidelines

Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems,
ii. Should be a mix of alphabets and numerical,
iii. Not be a dictionary word or proper name,
iv. Not be the same as the User ID,
v. Expire within a maximum of 90/120 calendar days,
vi. Not be identical to the previous password,
vii. Not be displayed on screen when entered,
viii. Ensure passwords are only reset for authorized user.

4.3 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, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

4.4 Password Protection

Here is a list of "do not's" for users so as to ensure Password Protection

- Don't reveal a password in an email message
- 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/friends/colleagues/others.
- Don't reveal a password to a co-worker while on vacation
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on any computer system unencrypted.

If someone demands a password, refer them to this document.

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

5. Penalties

Any employee found to have violated this policy may be subject to disciplinary action.

6. Review of the Policy

The Company is required to review the above policy in every two years based on its own experience, business need and RBI guidelines in this regard.