ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

PASSWORD POLICY

Version	2024/01.02
Review Date	05/04/2024
Review & Approved by	Reviewed by Technology Committee & Approved by Board of Directors

1 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 the compromise of company's entire corporate network. As such, all employees (including contractors and vendors with access to company's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. 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. Access to the resources on the network must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised

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) on any system that resides at company's any facility, has access to the company's network, or stores any company's non public information. This shall also include Wireless Network also.

4 Policy

4.1 General

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

4.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every one month. The recommended change interval is every fourteen calendar days.

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

4.1.4 Passwords must not be mentioned into email messages or other forms of electronic communication.

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

4.2 Trading Application Password

4.2.1 System mandated changing of password when the user logons for the first time.

4.2.2 All admin level, system level shall store in a sealed envelope

4.2.3 Automatic disablement of password on entering erroneous password on three consecutive occasions.

4.2.4 Password shall be alphanumeric and neither only alpha nor only numeric.

4.2.5 Password shall be change at an interval of fourteen calendar days.

4.2.6 Password shall not be same as last eight passwords.

4.2.7 Password shall not be same as User Login ID.

4.2.8 Password shall be at least six characters long and not more than twelve characters.

4.2.9 Password shall be automatically disabled on entering erroneous password on three continuous occasions.

5 Guideline

5.2 General Password Construction Guidelines

Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, 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.

5.1.1 Characteristic of Poor / Weak Password –

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.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, asdf1234, 123456 etc.
- Any of the above spelled backwards.

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. Outlook Express, Netscape 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 month. The recommended change interval is every fourteen calendar days.

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

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

6 Enforcement

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

7 Review and Update

This policy shall be reviewed and updated on an annual basis or on any special event or circumstance.