Account Password Policy

ITP Number ITP-SYS002	**Effective Date** February 20, 2005
Category IT Security Systems Management	**Supersedes** None
Contact it@pttuntex.com	**Scheduled Review** December 2023

PURPOSE

The purpose of this standard is to establish requirements for Tuntex company, staff and other users regarding passwords in order to protect individual and Tuntex information resource. Adherence to this standard will help ensure that Tuntex network and information systems are secure and available to all authorized users.

SCOPE

The scope of this standard includes all Tuntex employee, staff, and all authorized users who have or are responsible for an account on any system housing Tuntex information or that has access to the Tuntex network. Each user and/or system administrator on Tuntex network is required to implement the password requirements listed in this document.

CONTACTS

Direct any general questions about this standard to your unit's Tuntex Information Security Liaison. If you have specific questions, please contact ITS Information Security Compliance at it@pttuntex.com

Policy

All Tuntex-affiliated passwords should meet the requirements described below

All passwords used must be strong passwords. Passwords must be constructed using the following:

- minimum of eight (8) characters in length contains at least one character from each of the following four group:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Special character from this list ! * + - / _

- Passwords must expire within an appropriate interval. The default is 365 days for Tuntex employees, users, and other authorized individuals, if two-factor authentication is used. Without two-factor authentication, the default is 90 days. Some exceptions may apply, based on the individual's functional responsibilities.

- Password System Requirements:

    - The system must enforce the use of individual user IDs and passwords to maintain accountability.
    - The system must allow users to select and change their own passwords and include a confirmation procedure to allow for input errors.
    - The system must not display passwords on the screen when being entered.
    - The system must store and transmit passwords in protected.

- privileged Accounts

A privileged account has elevated permissions within a system that are significantly greater than those assigned to the majority of users. Privileged accounts should comply with the standard password requirements, expire every 90 days, and be audited at least annually.

Tuntex IT Division

Signature_____Annual Review Date _____