Connected Pakistan Password Policy

1. Purpose of This Policy

This policy outlines the requirements for creating and managing passwords at Connected Pakistan. Strong passwords are your first line of defense against unauthorized access to company data, systems, and client information. A robust password policy protects not only the company but also every individual employee. This policy was made after conducting an interview with non technical staff of Connected Pakistan for his password policy, it was also based on the observation of the auditors during their visit.

2. Key Principles of Strong Passwords

A strong password is:

- **Long:** The longer, the better.
- **Complex:** Uses a mix of different character types.
- **Unique:** Not reused across different accounts.
- **Difficult to Guess:** Not based on personal information, common words, or predictable patterns.

3. Password Requirements

All Connected Pakistan employees must adhere to the following requirements for all company-related accounts (laptops, Wi-Fi, email, internal systems, cloud services, etc.):

3.1. Minimum Length

- Minimum 12 characters for all accounts.
- Minimum 16 characters for highly sensitive accounts (e.g., administrator accounts, financial systems, critical client databases).

3.2. Complexity

Passwords must include at least three of the following four character types:

- Uppercase letters (A, B, C...)
- Lowercase letters (a, b, c...)
- Numbers (0, 1, 2...)
- Special characters (!, @, #, $, %, ^, &, *, etc.)

3.3. Uniqueness

- **Do NOT (Never)** reuse passwords. Each company account (email, Wi-Fi, internal system, etc.) must have a unique password.
- **Do NOT (Never)** reuse company passwords for personal accounts.

3.4. Password Changes

- Change passwords immediately if you suspect they have been compromised or if requested by IT.
- For less sensitive accounts, consider changing passwords every 90-180 days. For critical accounts, consider a shorter cycle or rely more heavily on Multi-Factor Authentication (MFA) and strong monitoring.

3.5. Handling & Storage

- Never write down passwords on sticky notes, whiteboards, or easily accessible places.
- Never share your password with anyone, including colleagues or IT support. IT will never ask for your password directly.
- Consider using a secure password manager (software designed to store and generate strong, unique passwords securely) if approved by management.

4. Multi-Factor Authentication (MFA)

- MFA (also known as 2-Factor Authentication or 2FA) such as Google Authenticator is mandatory wherever available. This adds an extra layer of security (e.g., a code from your phone, a fingerprint) beyond just your password.

- Always enable MFA for email, cloud services, and any internal systems that support it.

5. Best Practices for Employees

- **Think Passphrases:** Instead of a single word, create a phrase that is easy for you to remember but hard for others to guess. (e.g., MyDogLovesBones!2025).
- **Avoid Personal Information:** Do not use names, birthdays, pet names, or any easily discoverable information.
- **Avoid Common Words & Company-Related Terms:** Do not use dictionary words, common sequences (e.g., password123, qwerty), or terms directly related to the company (e.g., "Pakistan", "Connected", "CP", company names, product names, or service names).
- **Be Vigilant:** Always check the URL before entering credentials. If something looks suspicious, report it to management/IT.

6. Management & IT Responsibilities

- Implement technical controls to enforce this policy (e.g., system settings for minimum length, complexity, and lockout policies).
- Provide secure password management solutions or recommendations.
- Educate employees regularly on password best practices and phishing awareness.
- Monitor for suspicious login attempts and compromised accounts.
- This policy aims to significantly enhance Connected Pakistan's security posture by establishing clear, actionable guidelines for password management.