PASSWORD CREATION

To ensure the security of your passwords, follow these guidelines:

Complexity: Create passwords that are complex and difficult for others to guess.

Length: Passwords should be a minimum of eight characters and include a combination of lowercase and uppercase letters, numbers, and special characters.

Avoid Common Combinations: Exercise good judgment and avoid using basic combinations that may be easily guessed by others.

Unique Passwords: Each account should have a unique password. Avoid reusing passwords across different accounts or platforms.

Immediate Change: If a password's security has been compromised, change it immediately.

Regular Updates: Change passwords every 90 days to enhance security.

Ensuring Password Protection:

To protect your passwords, consider the following measures:

Confidentiality: Keep your passwords confidential and do not share them with anyone else.

Phishing Awareness: Stay vigilant against phishing scams and other fraudulent attempts to steal corporate credentials. Regular training and refresher courses will be provided to enhance awareness.

Avoid Writing Down Passwords: It is best to memorize passwords and avoid writing them down. This reduces the risk of physical compromise.

Approved Password Managers: If you prefer to use a password manager system, choose one that is approved by the device and ensure it is installed on your machines by authorized personnel.