CYBERDI

CMMC

CYBERDI

Password Policies and Procedures

CMMC Requirements

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

Non-Federal Organizations Tailor Password Policies to their Needs

Say what you do, explain how you do it, prove it gets done.

Do you enforce Complexity?

DoD nor NIST publishes requirements for complexity or resetting

Just Guidance

NIST Handbook 162 = 12 characters
.NIST SP 800-63B =8 characters
DoD =15 characters, combo of capital and special characters no MFA

Password or Passphrase?

Length beats complexity. If users need to remember a passowrd include passphrases in your policy

Do you require Resetting?

Explain in policy if you require periodic resetting.
Make employees change passwords on reset

NIST Recommends getting rid of password complexity and expirations policies

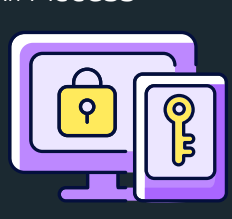
No adding or changing one character to an old password

Do you use Multi-Factor Authentication?

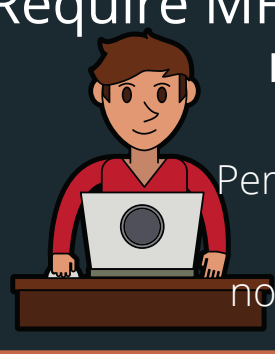
Many CMMC Practices Require MFA

Privileged Users
Perform security or duties abiove normal employees

< MFA All Access



MFA Network Acccess >



Non-Privileged Users
Perform security or duties abiove normal employees

Can you Use a Password Manager?

The discussion section in NIST 171 seems to negate use of modern password manager technologies.
YOU CAN AND SHOULD USE PASSWORD MANAGERS

Think About Your Traing Program!!