[Insert Company Name and Logo]	
Title: Authentication and Password Policy	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy establishes standards for creation of strong passwords, the protection of those passwords, and the frequency for changing those passwords. It is the policy of [Insert company name] to move toward multi-factor authentication of all users beginning with those accounts with privileged access and external access to the internal network.

Scope: This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) working in all facilities under the organization's ownership.

Policy:

1. Password construction
    a. All passwords must conform to this policy.
    b. Users must use differing passwords across all accounts.
    c. Users must not use the same passwords for [Insert Company name] accounts as they use for their personal accounts.
    d. Each user's password should meet the minimum requirements as outlined below (determine which requirements your organization will use):
        i. Must be a minimum of eight characters in length.
        ii. Must contain a unique character.
        iii. Must contain a number.
        iv. May not contain your username or any part of your full name
        v. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
    e. Passphrases are better used than passwords. (Example: BoilerUP! Can be converted to B01l@rUP!)
2. Password change (determine which requirements your organization will use)
    a. All passwords will be changed every 90 days.
    b. If a password is compromised, the Security Officer will be notified, and the password will be changed immediately.
    c. Users may not reuse the last five passwords.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

3. Password protection
    a. Passwords must not be shared with anyone.
    b. Do not write down passwords and do not post them anywhere.
    c. Do not store passwords in documents that are not encrypted.
    d. Do not use the “remember password” feature on applications.
    e. Do not send passwords through email.
    f. Do not reveal passwords over the phone.

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

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.