**Password Policy**

**Objective:** Create a **Password Policy** to ensure strong authentication practices and prevent unauthorized access.

**Understand Password Best Practices**:

**1. Purpose:** The purpose of this policy is to outline the best practices and guidelines for password management, with the goal of preventing unauthorized access to the organization's systems and data. By implementing strong password policies, we aim to mitigate the risks associated with weak passwords and reduce the likelihood of security breaches.

**2. Scope:** This policy applies to all employees, contractors, and interns who have access to company systems, applications, and network resources.

**3. Password Best Practices**

**a. Common Password Vulnerabilities:**

* **Weak passwords:** Passwords that are easy to guess or crack are a common vulnerability. These may include simple words, common phrases, or sequential characters.
* **Password reuse:** Using the same password across multiple platforms or systems increases the risk of compromise if one system is breached.

**b. Password Strength Requirements:**

* **Minimum length:** Passwords must be at least 12 characters in length.
* **Complexity:** Passwords must include a combination of at least three of the following:
  + Uppercase letters
  + Lowercase letters
  + Numbers
  + Special characters (e.g., !, $, @, #)
* **Expiration:** Passwords must be changed every 90 days. Notifications will be sent before expiration to ensure timely updates.
* **Multi-factor authentication (MFA):** MFA is mandatory for accessing sensitive or critical systems. Users must use a second factor (e.g., an authentication app, SMS code, or hardware token) alongside their password.

**c. Industry Standards:**

* This policy adheres to the NIST (National Institute of Standards and Technology) guidelines for password management, which recommend using strong, unique passwords and MFA to enhance security.

**4. Drafting a Password Policy**

**a. Password Complexity Requirements:**

* All passwords must meet the following criteria:
  + A minimum length of 12 characters.
  + A mix of uppercase and lowercase letters, numbers, and special characters.

**b. Password Management Guidelines:**

* **Regular password changes:** Users must change their passwords every 90 days.
* **Prohibition of password reuse:** Users are not permitted to reuse any of their last 5 passwords.
* **Password storage:** Passwords should never be written down or shared. Use secure password managers for storing passwords.

**c. Multi-factor Authentication (MFA):**

* MFA must be enabled for all accounts accessing sensitive company data, systems, or networks.
* Approved MFA methods include:
  + Authentication apps (e.g., Google Authenticator, Authy)
  + Hardware tokens
  + Biometric authentication (where available)

**d. Secure Password Storage:**

* Password managers must be used to store passwords securely. These tools encrypt passwords and require a master password for access.

**5. Case Study – Review and Policy Update**

**Quantum Lab, Hypothetical Company Review:**

* **Current Practices:**
  + Quantum Lab currently allows passwords with a minimum length of 6 characters.
  + Employees are not required to change passwords regularly.
  + MFA is not enforced for access to critical systems.
  + Some users store passwords in plain text or insecure systems.
* **Identified Weaknesses:**
  + Weak password length and complexity requirements.
  + Lack of password expiration and MFA implementation.
  + Insecure password storage practices.

**Policy Update:**

* **New Password Requirements:**
  + Passwords must be at least 12 characters long and include a mix of characters.
* **Mandatory MFA:**
  + Enforce MFA for all employees accessing sensitive systems or information.
* **Password Management Tools:**
  + Recommend the use of password managers and prohibit writing down or sharing passwords.
* **Periodic Reviews:**
  + Password policies will be reviewed annually to ensure alignment with industry standards and evolving threats.

**6. Enforcement:**

**Non-compliance with this policy will result in disciplinary action, which may include restricted access to systems, retraining, or termination of employment, depending on the severity of the violation.**

**End of Policy**

* Credential Stuffing Attack: **80% of hacking-related breaches** involve **passwords**.
* Password Guessing Attack: **81% of hacking-related breaches** are due to weak or stolen passwords.
* Data Breachs: In 2022, over **15 billion credentials** were exposed through data breaches. Many of these breaches occurred due to weak or reused passwords.