Password Policy

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

Steps:

1. **Understand Password Best Practices**:
    - Discuss common password-related vulnerabilities (e.g., weak passwords, password reuse).
    - Explain **password strength requirements** (e.g., length, complexity, expiration, and multi-factor authentication).
    - Review industry standards (e.g., NIST guidelines for password management).

2. **Drafting a Password Policy**:
    - Interns will create a **Password Policy** that includes:
        - Password complexity requirements (e.g., minimum length, use of special characters).
        - Guidelines for password management (e.g., regular password changes, prohibiting password reuse).
        - Recommendations for using **multi-factor authentication (MFA)** and secure password storage (e.g., password managers).

3. **Case Study**:
    - Review any company's current password management practices (a hypothetical scenario) and identify weaknesses. Then, update the policy to align with best practices.

Deliverables:

- A **Password Policy** document with clear guidelines for creating, storing, and managing passwords.
- A **'Google Slide'** short presentation on why strong password practices are essential to cybersecurity.