Here’s your **comprehensive sentence-by-sentence breakdown** of the Password Best Practices document, formatted for professional Word usage with numbering, minimal spacing, and detailed explanations for clarity.

**Password Best Practices – Detailed Study Notes**

1. **Overview of Password Best Practices**
   * Covers password **complexity requirements**, **expiration requirements**, and **BIOS/UEFI password usage**.
   * Passwords are one of the most common security measures across websites, applications, and operating systems.
   * Authentication can use traditional passwords, PINs, or combinations of both.
2. **Password Weakness & Attacks**
   * Passwords and PINs are considered **weak authentication** because they can be cracked.
   * Common password attack methods: **brute force**, **dictionary**, and **hybrid attacks**.
   * Despite weaknesses, passwords remain widely used—administrators must enforce strong policies.
3. **Creating Stronger Passwords via Policies**
   * Goals:
     + Use **long, complex passwords**.
     + Implement regular **password expiration**.
   * Configured through **Group Policy** in Windows:
     + Path: *Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy*.
     + Options include minimum password length and enabling complexity requirements.
4. **Password Length**
   * Minimum password length example: 12 characters (can be set from 8 to 14 in Windows 10+).
   * Longer passwords drastically improve security due to the exponential increase in possible combinations.
5. **Password Complexity: About how difficult it is going to be to create that password based on the type of characters that can be used.**
   * Complexity is determined by the range of characters allowed:
     + Numbers only: 10 possibilities per character (0–9). Example: 4-digit PIN = 10,000 possible combinations.
     + Lowercase letters only: 26 possibilities per character.
     + Lowercase + uppercase: 52 possibilities.
     + Adding numbers: 62 possibilities.
     + Adding special characters: ~75 possibilities.
   * Example:
     + 4 characters using 75 options = 75⁴ = 31,640,625 combinations.
       1. 75 x 75 x 75 x 75
       2. Pin1 x pin2 x pin3 x pin4
     + Increasing length to 5 characters with same complexity = over 2 billion combinations.
       1. 75 x 75 x 75 x 75 x 75
       2. Pin1 x pin2 x pin3 x pin4 x pin5
6. **Importance of Combining Length & Complexity**
   * Length alone (e.g., a 10-digit phone number) without complexity still yields a limited set of combinations.
   * Best practice: combine both for maximum strength.
   * Recommended minimum: **12+ characters** using uppercase, lowercase, numbers, and special characters.
7. **Password Expiration & Age**
   * Policies include **maximum password age** (expiration) and **minimum password age** (prevents immediate reuse).
   * Example: 90-day maximum age forces a password change every three months.
   * Older guidance favored frequent changes; newer recommendations suggest keeping long strong passwords longer to avoid poor user practices (like writing them down).
8. **Passwordless Authentication Trends**
   * Alternative methods eliminate static passwords:
     + Example: Email-based one-time link login.
     + Risks: If email is compromised, access is also compromised.
   * Still requires strong security on the alternate authentication method.
9. **Best Practice for Expiration Intervals**
   * Recommended: 90-day rotation for strong, complex passwords.
   * Combined with **two-factor authentication (2FA)** for higher security:
     + Something you know (password) + something you have (token, authenticator app).
10. **BIOS/UEFI Password Protection**
    * BIOS (Basic Input/Output System) and UEFI (Unified Extensible Firmware Interface) control system startup before OS loads.
    * Protect BIOS/UEFI with strong passwords to:
      + Prevent unauthorized boot order changes.
      + Protect against tampering with critical system settings.
    * Use **long, complex passwords** for BIOS/UEFI to guard against guessing or brute force attacks.