Task 2

Password Policy:

Why is Password Policy? because Passwords are the first defence against unauthorized access. Strong, unique passwords that are updated regularly help lower the risk of attacks. Weak passwords can be easily cracked with brute-force attempts.

Creating Passwords:

Your password should be at least 12 characters long.

- It must include a combination of: uppercase and lowercase letters (A-Z, a-z), Numbers (0-9), Special characters (like !@#$%^&*)
- Don't use easy-to-guess information like your name, birthday, or common words like "password123."

Using Passwords:

- Use a different password for each system.
- Enable multi-factor authentication (MFA) whenever possible. This adds extra security beyond just the password.

Changing Passwords:

- Change your password every 90 days.
- Don't reuse any of your last 5 passwords.
- If you think your password has been stolen or hacked, change it right away.

Account Lockout:

- After 4 wrong password attempts, your account will be locked for 45 minutes.
- This helps prevent brute-force attacks, as suggested by NIST (National Institute of Standards and Technology).

Enforcement:

Not following this policy may result in disciplinary actions, including losing access privileges or even termination of employment.

References:

- NIST Special Publication 800-63: Digital Identity Guidelines
- NIST Special Publication 800-12: An Introduction to Computer Security
- NIST Special Publication 800-53: Security and Privacy Controls for Information Systems

Social Media Security Policy

What is the Purpose? this policy explains how employees should use social media in a way that protects the company's confidential information, brand, and reputation, while following legal and ethical rules. Social media is a powerful way to connect with the public, but it also brings serious risks to the company's reputation, data security, and legal standing. Phishing attacks, fake accounts, and leaking confidential information are common threats caused by careless social media use

Policy:

Scope: This policy applies to all employees, contractors, and anyone representing the company on social media, whether using personal or company accounts.

Personal Social Media Use:

- Employees must make sure their personal social media activity doesn't harm the company's image.
- Don't share any confidential company information (like financial data, projects in progress, or client details).
- If you talk about related work topics, make it clear that your opinions are personal and don't represent the company.

Official Social Media Use:

- Only authorized employees can post on the company's official social media accounts.
- Make sure that all posts are accurate.

Security Precautions:

- Use strong passwords (follow password policy on this link ……)
- Be careful of phishing attacks or suspicious links.

Prohibited Activities:

- Don't post any offensive or inflammatory comments that could damage the company's reputation.

Use of Personal Devices: You are not allowed to use your personal device to mange company social media accounts. You must use company`s device to do the work of the company, because all company`s devices protected with encryption and antivirus software

Enforcement: Failure to follow this policy can lead to disciplinary action, which may include being fired or facing legal consequences, depending on the severity of the violation.

Additional Tips:

- **Phishing:** Phishing is a type of cyberattack where someone pretends to be a trusted source to steal sensitive information.
- **Multi-Factor Authentication (MFA):** MFA is a security process where users must provide two types of identification before they can access their accounts.

References:

- NIST Special Publication 800-63: Digital Identity Guidelines

- ISO/IEC 27002: Code of Practice for Information Security Controls