TASK-2

Q) Create a password policy for a company that enforces strong and unique passwords.

Creating a strong and unique password policy is essential for enhancing security within your company. Here's a comprehensive password policy that you can implement:

Password Policy for [Company Name]

1. Password Complexity:

- Passwords must be at least 12 characters long.
- Passwords must include a combination of:
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (e.g., !, @, #, $, %, etc.).

2. Password Expiration:

- Passwords must be changed every 90 days.
- Users will be notified via email or system prompts to change their passwords when they are due for expiration.

3. Password History:

- Users cannot reuse their last 5 passwords.

4. Account Lockout:

- After 5 consecutive failed login attempts, the account will be locked for 30 minutes.
- Users must contact IT support to unlock their accounts after the lockout period.

5. Multi-Factor Authentication (MFA):

- MFA is required for all user accounts to add an extra layer of security. This can include SMS, app-based authentication, or hardware tokens.

6. Password Storage and Transmission:

- Passwords must be securely hashed and salted before storage.
- Passwords transmitted over the network must be encrypted using secure protocols (e.g., HTTPS).

7. User Education:

- Regular training and awareness programs must be conducted to educate users on the importance of strong passwords and the risks of sharing or writing down passwords.

8. Account Recovery:

- A secure and standardized account recovery process must be in place for users who forget their passwords.

9. Third-party services:

- When third-party services are used, their password policies and security measures should be reviewed and aligned with the company's password policy.

10. Password Manager Recommendations:

- Encourage users to utilize a password manager to securely store and generate strong, unique passwords.

11. Password auditing:

- Periodic audits should be conducted to ensure compliance with the password policy.

12. Reporting Security Concerns:

- Users should be encouraged to report any security concerns or suspicious activity related to their accounts.

13. System Access Review:

- Regularly review and update access privileges to ensure that users have the necessary permissions and nothing more.

14. Password Reset Procedure:

- Establish a secure procedure for users to reset their passwords if they forget them.

15. Monitoring and Logging:

- Maintain logs of login attempts and password changes, and regularly monitor for unusual or unauthorized activity.

16. Enforcement:

- Non-compliance with this policy may result in disciplinary action, including account suspension or termination.

17. Review and Revision:

- Regularly review and update the password policy to adapt to evolving security threats and industry best practices.

By implementing this comprehensive password policy, your company can significantly enhance security by ensuring strong and unique passwords while promoting best practices in password management.