US Solutions Pvt Ltd. - Password Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 03/01/2025
- **Author:** IT & Infosec Department
- **Approved By:** Manager
- **Effective Date:** 03/01/2025
- **Review Frequency:** Annually

1. Introduction

At US Solutions Pvt Ltd., the security of our information assets is paramount. Passwords serve as a critical first line of defense against unauthorized access. This Password Policy establishes the minimum standards and guidelines for creating, managing, and protecting passwords across all Company systems and applications. All employees, contractors, and authorized users ("Users") are required to adhere to this policy to ensure the confidentiality, integrity, and availability of our data.

2. Purpose

The purpose of this policy is to:

- Establish a robust framework for password management.
- Minimize the risk of unauthorized access to Company systems and data.
- Promote a culture of security awareness among Users.
- Ensure compliance with industry best practices and applicable regulations.

3. Scope

This policy applies to all Users who access Company IT resources, including but not limited to:

- Company workstations and laptops.
- Network accounts and servers.
- Email and messaging systems.
- Cloud-based applications and services.
- Mobile devices used for Company business.
- VPN and remote access systems.
- All other systems requiring authentication.

4. Password Requirements

All passwords must adhere to the following minimum requirements:

- **Length:** Passwords must be a minimum of 12 characters.
- **Complexity:** Passwords must include a combination of:
  - Uppercase letters (A-Z).
  - Lowercase letters (a-z).

    - Numbers (0-9).
    - Special characters (!@#$%^&*()-_=+[{]};:'",<.>/?).
- **Uniqueness:** Passwords must not be reused across multiple systems or accounts.
- **Avoidance of Personal Information:** Passwords must not contain easily guessable information, such as:
    - Usernames, employee IDs, or company names.
    - Personal names, dates of birth, or addresses.
    - Common words or phrases found in dictionaries.
- **Password History:** Users must not reuse any of their previous 5 passwords.

5. Password Management

- **Password Changes:** Users are required to change their passwords at least every 90 days.
- **Password Storage:** Passwords must never be written down or stored in plain text. Users are encouraged to use a reputable password manager.
- **Password Sharing:** Passwords must not be shared with anyone, including colleagues or IT support personnel, unless explicitly authorized by senior management for a specific, documented business need.
- **Account Lockout:** After a specified number of failed login attempts (e.g., 5), accounts will be locked for a defined period (e.g., 30 minutes).
- **Password Recovery:** Users must utilize the Company's designated password recovery procedures. IT support will verify the identity of the user before resetting passwords.

6. Multi-Factor Authentication (MFA)

- MFA is mandatory for all access to sensitive systems and applications, including but not limited to VPN, email, and cloud services.
- Users must enroll in the Company's approved MFA solution.
- Users are responsible for maintaining the security of their MFA devices and credentials.

7. Responsibilities

- **Users:**
    - Comply with this Password Policy.
    - Create and maintain strong, unique passwords.
    - Protect their passwords from unauthorized access.
    - Report any suspected password compromises to the IT department immediately.
    - Enroll and use MFA as required.
- **IT Department:**
    - Enforce this Password Policy.
    - Provide guidance and support to Users on password management.
    - Maintain and monitor password security systems.
    - Investigate and respond to password-related security incidents.
    - Ensure MFA systems are running and available.
- **Managers:**

    - Ensure that their teams are aware of and comply with this Password Policy.
    - Report any password-related security concerns to the IT department.
    - Support the IT departments security initiatives.

8. Policy Enforcement

- Failure to comply with this Password Policy may result in disciplinary action, up to and including termination of employment or contract.
- The IT department will conduct regular audits to ensure compliance with this policy.
- Any suspected password compromises will be investigated thoroughly.

9. Exceptions

- Any exceptions to this policy must be approved in writing by the Chief Information Security Officer (CISO) or designated authority.
- Exceptions will be granted only for specific, documented business needs and will be subject to appropriate security controls.

10. Training and Awareness

- All new Users will receive training on this Password Policy as part of their onboarding process.
- Regular security awareness training will be provided to all Users to reinforce password security best practices.
- The IT department will provide documentation and resources to assist users with password management.

11. Review and Updates

- This Password Policy will be reviewed and updated annually, or more frequently as needed, to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

12. Reporting Security Incidents

- Users must immediately report any suspected or actual password compromises or security incidents to the IT department.
- Reports should include as much detail as possible, including the date, time, and nature of the incident.

13. Password Manager Best Practices.

- Company recomends the use of a company approved password manager.
- Users are responsible for the master password, and ensuring it meets all policy requirements.
- Users must back up their password manager data.
- Users must not store company passwords in any other location outside of the password manager.

This Password Policy is essential for maintaining the security of US Solutions Pvt Ltd.'s information assets. By adhering to these guidelines, Users contribute to a safer and more secure work environment.