Password Policy

1. Purpose:

The purpose of this Password Policy is to ensure the security and confidentiality of RampedUp's information and associated assets by establishing guidelines for creating strong and secure passwords.

2. Scope:

This policy applies to all employees, contractors, vendors, and any other individuals granted access to our organization's systems, networks, and data.

3. Password Creation:

- Passwords must be at least 12 characters long.

- Passwords should include a mix of uppercase and lowercase letters, numbers, and special characters.

- Passwords should not contain easily guessable information, such as common words, birthdates, or easily accessible personal details.

4. Password Complexity:

Passwords should meet a minimum complexity score, as determined by the organization's password management tool or policy.

5. Password Expiration and History:

- Passwords should be changed every 90 days.

- Users cannot reuse their last 5 passwords.

6. Password Storage and Transmission:

- Passwords must not be stored in plain text format.

- Passwords must not be sent via email or other insecure communication channels.

7. Multi-Factor Authentication (MFA):

- Multi-Factor Authentication is required for all accounts accessing sensitive or critical systems and data.

- MFA should be enabled using approved and secure methods such as tokens, SMS, or authenticator apps.

8. Account Lockout and Brute-Force Protection:

- After 10 failed login attempts, the account should be locked for a specified duration.

- Brute-force attacks on login credentials are strictly prohibited.

9. Password Sharing and Management:

- Users must not share their passwords with anyone, including colleagues or IT staff.

- Users must not write down their passwords or store them in easily accessible places.

- Passwords must be kept confidential at all times.

10. Password Reset and Account Recovery:

- Users should follow the organization's prescribed procedures for password reset and account recovery.

- Account recovery processes should be secure and require additional verification to prevent unauthorized access.

11. Third-Party Passwords:

- Users must not reuse their work-related passwords for personal accounts or third-party services.

- Separate passwords should be used for personal and work-related accounts.

12. Training and Awareness:

- Regular security awareness training should be provided to all users to educate them about the importance of strong passwords and the risks of weak passwords.

13. Password Policy Compliance:

- IT administrators must monitor password compliance and take appropriate action against users who violate the policy.

- Non-compliance with the password policy may result in disciplinary action.

14. Review and Updates:

- This Password Policy will be periodically reviewed to ensure its relevance and effectiveness, considering changes in technology and security threats.

By adhering to this Password Policy, all users contribute to the protection of our organization's sensitive information and assets. Failure to comply with this policy may result in loss of access privileges, disciplinary action, or legal consequences.