

**Purpose:** This policy outlines Steve J Martin Ltd's requirements for creating and using strong passwords to protect our information assets.

**Scope:** This policy applies to all employees, contractors, and visitors who have access to our information systems.

**Policy Statement:** Steve J Martin Ltd is committed to protecting our information assets from unauthorized access. Strong password management is a critical component of our cybersecurity strategy.

#### Password Requirements:

- Length: Passwords must be at least [number] characters long.
- Complexity: Passwords must contain a combination of uppercase and lowercase letters, numbers, and special characters.
- Uniqueness: Passwords must be unique and not reused across different accounts.
- Avoidance of Personal Information: Passwords should not contain easily guessable information, such as personal names, birthdays, or pet names.

#### Password Change:

- Employees must change their passwords regularly, at least every 3 months.
- Passwords should be changed immediately if they are suspected of being compromised.

#### Password Storage:

- Passwords will be stored in a secure, encrypted format.
- Plaintext passwords will never be stored.

#### Password Sharing:

- Employees are prohibited from sharing their passwords with others.
- If a password is shared with another employee, it must be changed immediately.

#### Phishing Awareness:

- Employees will be trained to recognize and avoid phishing attempts.
- Phishing attempts should be reported immediately to the IT department.

**Responsibilities:**

- **Management:**
  - Develop and implement password policies and procedures.
  - Ensure that employees are aware of and comply with password requirements.
  - Monitor password usage and enforce policies.
  - Investigate password-related incidents.
- **IT Department:**
  - Implement technical measures to protect passwords.
  - Provide training and support to employees on password management.
  - Investigate password breaches and take appropriate action.
- **Employees:**
  - Comply with password policies and procedures.
  - Use strong, unique passwords.
  - Report any suspicious password activity.

**Review and Improvement:**

- This policy will be reviewed annually to ensure its effectiveness.
- Continuous improvement measures will be implemented to enhance our password management practices.

Steve Martin  
Company Director

*Steve Martin*