Password Creation and Management Policy

Purpose: The purpose of this policy is to establish guidelines for creating and managing passwords to ensure the security of our company's information and assets.

Policy:

1. Password Creation:

a. Passwords must be a minimum of 8 characters long.

b. Passwords must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

c. Passwords must not contain any dictionary words, names, or any easily guessable information such as birthdates or phone numbers.

d. Passwords must be unique and not used for any other accounts or services.

e. Passwords must be changed every 90 days.

f. Passwords must never be shared with anyone, including IT support staff.

1. Password Management:

a. Passwords must be stored securely and never be written down on paper or stored in plain text.

b. Passwords must not be saved in web browsers or any software that can store passwords.

c. Users should log out of their accounts when they are finished working and never leave their computers unattended while logged in.

d. Passwords must be reset immediately if they are suspected of being compromised or if there is any suspicion of unauthorized access.

e. Users should use a different password for each account or service to prevent unauthorized access to multiple accounts in case of a password breach.

f. Multi-factor authentication should be used wherever possible to add an extra layer of security to the authentication process.

1. Password Requirements for Third-party Vendors:

a. All third-party vendors that have access to our company's information or systems must adhere to the same password creation and management policy as our employees.

b. Third-party vendors must use unique passwords for accessing our systems and must never share passwords with anyone, including IT support staff.

c. Third-party vendors must notify us immediately if they suspect that their password has been compromised.

Enforcement: Violation of this policy may result in disciplinary action, up to and including termination of employment or contract. It is the responsibility of each employee, contractor, and third-party vendor to adhere to this policy.

Review: This policy will be reviewed and updated annually or as needed by the IT department.