**Information Security Policy: Password Policy**

**Policy Statement:**

To ensure the security of company systems and data, a robust password policy is in place. This policy aims to establish guidelines for creating and managing passwords to prevent unauthorized access, protect sensitive information, and maintain the confidentiality of our digital assets.

**1. Password Complexity Requirements:**

a. **Minimum Length:** Passwords must be a minimum of 12 characters in length.

b. **Complexity:** Passwords must include a combination of the following elements:

* Uppercase letters
* Lowercase letters
* Numbers
* Symbols or special characters

**2. Password Management:**

a. **Password Change:** Users are required to change their passwords at least every 6 months.

b. **No Password Reuse:** Users are prohibited from reusing passwords. Each new password must be unique and not resemble any of the user's previous passwords.

**3. Password Security Practices:**

a. **No Sharing:** Users are strictly prohibited from sharing their passwords with anyone, including colleagues, family members, or external parties. Each individual must have their unique set of credentials.

b. **Confidentiality:** Users must treat their passwords as confidential information and must not write them down or store them in easily accessible locations.

c. **Unauthorized Access:** Users must report any suspected or actual unauthorized access to their accounts promptly to the IT department.

**4. Multi-Factor Authentication (MFA):**

a. **Use of MFA:** Where applicable, users are encouraged to enable multi-factor authentication for an additional layer of security.

**5. Password Recovery:**

a. **Authorized Channels:** Password recovery or reset requests should only be made through authorized channels provided by the IT department. Users should never share their passwords via email or other unsecured communication methods.

**6. Policy Enforcement:**

a. **Monitoring:** The IT department may monitor password usage and conduct periodic assessments to ensure compliance with this policy.

b. **Non-Compliance:** Failure to comply with this password policy may result in consequences, including account suspension, access restrictions, or other disciplinary actions.

**7. Policy Review:**

This policy will be subject to periodic review and updates to align with industry best practices and emerging cybersecurity threats.

**Acknowledgment:**

By using company systems and services, users acknowledge their understanding of and commitment to complying with this password policy.

*Date of Policy Implementation: (DATE)*

*Policy Owner: (COMPANY NAME)*