PASSWORD POLICY CHECKLIST

GIBRALTAR®
gibraltarsolutions.com

Password Creation

- □ Create strong passwords that are at least 14 characters long
- □ Include a mix of uppercase and lowercase letters, numbers, and special characters in your password
- □ Avoid using easily guessable information, such as names, birthdays, or common words
- □ Do not use dictionary words or everyday phrases
- □ Consider using passphrase-style passwords, which are longer and easier to remember
- □ Do not reuse old passwords
- □ Screen passwords against commonly used and breach password lists

Password Management

- □ Use unique passwords for each account or system
- □ Do not share your password with anyone, including coworkers or IT personnel
- □ Never write down your passwords or store them in an easily accessible location
- □ Use a password manager to store and generate complex passwords securely
- □ Be aware of password expiration periods and change your password as required
- □ Change your password immediately if you suspect it has been compromised

Multi-Factor Authentication

- □ Enable multi-factor authentication wherever possible to add an extra layer of security
- □ Use a secure MFA method, such as a mobile app or hardware token, rather than SMS-based authentication

Password Reset

- □ Follow your organization's password reset procedures when required
- □ Verify the authenticity of password reset emails or messages to avoid phishing attempts

Account Lockout

- □ Do not attempt to guess other users' passwords or engage in unauthorized access
- □ Understand the organization's account lockout policy and avoid triggering it accidentally

Reporting Incidents

- □ Report any suspicious activity involving your password immediately to the IT department