PASSWORD POLICY

DATE: FEBRUARY 5, 2016

1. Overview

All customers and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

2. Password Protection

- Never write passwords down.
- Never send a password through email.
- Never include a password in a non-encrypted stored document.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Never hint at the format of your password.
- Never reveal or hint at your password on a form on the Internet.
- Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
- Never use your corporate or network password on a Non-Cameo site.
- Report any suspicion of your password being broken to management.
- If anyone asks for your password, refer them to management.
- Don't use common acronyms as part of your password.
- Don't use common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.

3. Password Requirements

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess.

The following password requirements will be utilized by Cameo customers:

- Minimum Length - 7 characters
- Minimum complexity Suggestions- No dictionary words included. Passwords should use three or four of the following four types of characters:
- Lowercase
- Uppercase
- Numbers
- Special characters such as !@#$%^&*(){}[]
- Passwords are case sensitive and the user name or login ID is not case sensitive.
- Password history - 24 (Required number of unique passwords before an old password may be reused)
- Maximum password age - 90 days
- Minimum password age - 2 days
- Account lockout threshold - 3 failed login attempts

- Reset account lockout after – 30 minutes (Time it takes between bad login attempts before the count of bad login attempts is cleared)
- Account lockout duration – 30 minutes (Determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked)
- Rules that apply to passwords apply to passphrases which are used for public/private key authentication

4. Choosing Passwords

Users are instructed to avoid creating passwords that use:

- Dictionary words in any language.
- Words spelled backwards, common misspellings, and abbreviations.
- Sequences or repeated characters Personal information. Your name, birthday, driver's license, passport number, or similar information.

5. Revision History

Date of Change	Version	Responsible	Summary of Change
1/20/2016	1.0	DH	Document creation, initial policy definition
2/5/2016	1.1	DH	Format updated