8060.S000 Access Control - Appendix A

1.0 Examples of password management settings

1.1 Compliant examples of password criteria that Meet NIST Level 1 include but are not limited to:

a) 8 characters, with composition rules, no dictionary check, 90 day lifetime, 3 failed logins lock account for 25 minutes

b) 8 characters, with composition rules, no dictionary check, 180 day lifetime, 3 failed logins lock account for 50 minutes

c) 15 characters, no composition rules, no dictionary check, 180 day lifetime, 3 failed logins lock account for 30 minutes

1.2 Compliant examples of password complexity that meet NIST Level 1 include but are not limited to:

a) Minimum password length of eight (8) characters, password must contain at least three (3) out of the four (4) following character types:

- At least one uppercase alphabetic character (A-Z)
- At least one lowercase alphabetic character (a-z)
- At least one special character
- At least one number (0-9)

b) Minimum password length of fifteen (15) characters, password must use "pass phrase" composed of four (4) words and punctuation

1.3 Compliant examples of failed login attempt lockout settings include but are not limited to:

a) After 8 sequential failed authentication attempts, account is locked for 50 minutes

1.4 Compliant examples of password ageing re-use settings include but are not limited to:

a) Passwords protecting administrative access to Level 1 or Level 2 data must be changed every 90 days

β) Passwords protecting the ability to create application transactions (e.g. create and/or approve purchase requisitions, create general ledger transactions) must be changed every 180 days

χ) Password reuse must be restricted to no more than one in every four (4) password used.