Purpose:

To define minimum password complexity requirements based upon assigned password policy levels.

Standard:

1. Password construction attributes (Table 1) for each password policy level are selected to achieve the specified minimum entropy.

2. Password composition rules require the inclusion of 3 of the 4 following character sets: lowercase letters, uppercase letters, numerals and special characters. Allowable special characters are ~!@#$%^&*()_+|`-=\{}[]:";'<>?,./ and the space character (depending on system support). Passwords may not include words of more than 4 characters, as tested against a dictionary of at least 50,000 words.

3. For all policy levels, the selection of a passphrase of at least 18 characters eliminates the password composition rules and dictionary check. Passphrases are subject to minimal tests to prevent use of common or trivial phrases.

4. Multi-Factor Authentication (MFA) may be offered for use with policy levels P3-P5, and is required for P6

Standard Number:	Standard Family:	Category:	Effective Date:
SEC-AC-002.02	Information Security	Policy Category	6/24/2015

Revised:5/22/2015   Page **1** of **2**

Standard: Password Complexity

Table 1 – Password Construction Attributes

Attribute	P1	P2	P3	P4	P5	P6
Minimum entropy bits	30	30	30	31.5	31.5	31.5
Minimum length of password	8	8	8	9	9	9
Maximum age of password (in days)	365	365	365	180	180	90
Password minimum age for reset (in days)	1	1	1	1	1	1
Password uniqueness/history (days)	200	200	200	200	200	200
Failed attempts before lockout	10	10	10	10	10	6
Lockout duration (minutes)	30	30	30	30	30	30

References:

SEC-AC-002.01: Authentication Management Standard

NIST Special Publication 800-63 revision 1: Electronic Authentication Guideline

PCI Data Security Standard 2.0