UF UNIVERSITY of FLORIDA
Information Technology

Standard: Password Complexity

Purpose:

To define password policy levels based upon the level of system or data access granted to the account, and the complexity requirements associated with each.

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. Passwords may not include words greater 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 checks to prevent use of extremely simple or common character combinations and phrases.

4. Authentication token devices may be offered for use with policy levels P3-P5. When authentication token devices are used in conjunction with a password, the password is not required to comply with password construction attributes or composition rules.

Table 1 – Password Construction Attributes

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

References:

SEC-AC-002.01: Authentication Management Standard

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