UF UNIVERSITY of FLORIDA
Information Technology

Standard: Password Complexity

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. Two-Factor Authentication is required for policy level P6 and optional for all faculty, staff and affiliates. Faculty, staff and affiliates whose accounts are compromised will be required to enroll in Two-Factor Authentication.

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	365
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	10
Lockout duration (minutes)	30	30	30	30	30	30

References:

SEC-AC-002.01: Authentication Management Standard

NIST Special Publication 800-63-3: Digital Identity Guidelines

UF Two-Factor Authentication https://it.ufl.edu/two-factor