UF College of Pharmacy
UNIVERSITY of FLORIDA

Information Technology Department

Document Number:	IT-SEC-0006.001	**Document Name:**	Password Complexity Standard
Effective Date:	?	**Approval Date:**	?
Document Type:	Standard	**Page Count:**	3
Document Status:	?	**Document Category:**	IT – Security
Document Owner:	Lane Blanchard	**Document Version:**	1.4

1.0 Revision History

Version	Date	Author(s)	Change Description
0.0	7/15/2013	UF IT Security	Initial UF Document that was adopted.
1.0	10/17/2018	Lane Blanchard	First full document drafted from adopted document; Modifications for internal needs and requirements
1.1	12/15/2018	Lane Blanchard	None
1.2	11/05/2019	Lane Blanchard	None
1.3	01/15/2021	Lane Blanchard	Added two links to each Authentication Management Standard AND Policy
1.4	04/04/2023	Lane Blanchard	None

2.0 Policy Approval

Name of Approver: Shaima Coffey

Title of Approver: ISA and Executive Director

Approval Date: ?

UF College of Pharmacy
UNIVERSITY of FLORIDA

Information Technology Department

3.0 Purpose

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

4.0 Details

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

4.2 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.

4.3 For all policy levels, the selection of a pass-phrase 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.

4.4 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.

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 (in days)	200	200	200	200	200
Failed attempts before lockout	10	10	10	10	10
Lockout duration (minutes)	30	30	30	30	30

5.0 Scope

This policy applies to all passwords and other authentication methods used at the College of Pharmacy.

6.0 Related Policies

- ***IT-SEC-0006 Authentication Management Policy*** https://it.ufl.edu/policies/information-security/authentication-management-policy/

- ***IT-SEC-0006.002 Authentication Management Standard*** https://it.ufl.edu/policies/information-security/related-standards-and-documents/authentication-management-standard/

7.0 Definitions

No definitions needed for this standard.

8.0 Supporting Information

- NIST Publication 800-63 Electronic Authentication Guide