UF College of Pharmacy
UNIVERSITY of FLORIDA

Information Technology Department

Document Number:	IT-SEC-0006	**Document Name:**	Authentication Management Policy
Effective Date:	01/15/2021	**Approval Date:**	02-18-2021
Document Type:	Policy	**Page Count:**	3
Document Status:	Approved	**Document Category:**	IT – Security
Document Owner:	Lane Blanchard	**Document Version:**	1.3

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	10/17/2017	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 links to Authentication Management Standard and Password Complexity Standard
1.4	04/04/2023	Lane Blanchard	NONE. Verified Links

2.0 Policy Approval

Name of Approver: Ian Tebbett

UF College of Pharmacy
UNIVERSITY of FLORIDA

Information Technology Department

Title of Approver: Assoc. Dean, Entrepreneurial Programs and IT

Approval Date: 02-18-2021

3.0 Purpose

Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. It is essential that these authenticators be strongly constructed and used in a manner that limits their compromise.

4.0 Policy Details

4.1 General Rules

- 4.1.1 Access to all data and systems not intended for unrestricted public access requires authentication.
- 4.1.2 Passwords and other authenticators must be constructed to have a resistance to attack commensurate with the level of system or data access granted to the account.
- 4.1.3 Systems must be designed and configured to protect passwords during storage and transmission.
- 4.1.4 No one may require another to share the password to an individually assigned university account, for example as a condition of employment or in order to provide technical support.

4.2 Responsibilities

- 4.2.1 All members of the College of Pharmacy are responsible for any activity that occurs as a result of the use of authentication methods issued to them.
- 4.2.2 All members of the College of Pharmacy are responsible for protecting the password or authentication method associated with an individually assigned university account. Passwords may not be shared or disclosed to anyone else.
- 4.2.3 All members of the College of Pharmacy are responsible for reporting any suspicious use of assigned authentication mechanisms. Anyone that reasonably believes his or her password is known by anyone must change it immediately. Lost or stolen authentication devices are to be reported immediately to the College of Pharmacy Information Security Manager (ISM).
- 4.2.4 College of Pharmacy Information Security Manager (ISM), or their designee, is responsible for verifying that information systems under their control, and those intended for acquisition or development, comply with this policy.

5.0 Policy Compliance

5.1 Compliance Management

The College of Pharmacy Information Security Manager (ISM), or their designee, will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru inspections, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner and privacy committee.

5.2 Exceptions

The College of Pharmacy Information Security Manager (ISM), or their designee must approve any exception to the policy in advance.

5.3 Non-Compliance

An employee found to have violated this policy would be subject to disciplinary action, up to and including termination of employment.

6.0 Policy Scope

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

7.0 Related Policies

- ***IT-SEC-0006.001 Password Complexity Standard*** https://it.ufl.edu/policies/information-security/related-standards-and-documents/password-complexity-standard/
- ***IT-SEC-0006.002 Authentication Management Standard*** https://it.ufl.edu/policies/information-security/related-standards-and-documents/authentication-management-standard/

8.0 Definitions

No definitions applied to this policy.

9.0 Supporting Information

- NIST Publication 800-53 Security and Privacy Controls for Federal Information Systems & Organizations