UNIVERSITY OF DENVER	**UNIVERSITY OF DENVER** **POLICY MANUAL** **PASSWORD MANAGEMENT**	
Responsible Department: Information Security Office **Recommended By**: VC Information Technology, Chief Information Security Officer **Approved By**: Chancellor	**Policy Number** IT 13.01.013	**Effective Date** 1/11/2023

I. INTRODUCTION

Passwords and passphrases are an important tool in protecting the confidentiality, integrity, and availability of the University's information resources.

II. POLICY OVERVIEW

All members of the University community with access to the University's information systems are responsible for keeping passwords secure and confidential.

III. PROCESS OVERVIEW

A. Members of the University community who are granted access to the University's information resources are required to change the IT- assigned password immediately after receipt of such initial password. Initial passwords will be securely transmitted to the individual.

B. Passwords and passphrases should never be shared with another individual for any reason or in any manner not consistent with this Policy.

C. University password/passphrases should be unique and used only to access University resources (i.e. University passwords should not be re-used to login to third-party sites or resources (ex. Gmail or Yahoo password, Facebook or Twitter password, etc.).

D. Passwords/passphrases should not be written down. The University will provide a secure password manager for University community members use.

E. Password Requirements

1. Passwords/passphrases must be a minimum of fifteen (15) characters.
2. Passwords/passphrases expiration shall be set to 365 days for non-MFA enabled accounts, for MFA-enabled account, a password/passphrase reset is only required upon potential or confirmed password compromise.
3. Passwords/passphrases shall lock after five (5) failed attempts. Automatic reset shall be set at five (5) minutes.
4. Passwords/passphrase history shall be set to last eight (8) passwords and the same password/passphrase cannot be re-used within the last two (2) years.
5. Users shall be notified at least two (2) weeks before their password/passphrase is about to expire.
6. When a password/passphrase reset is requested, the reset request will not be processed until the individual has been verified.

F. Exceptions

1. Any exception to this Policy must be approved in writing by the University's Chief Information Security Office (CISO).
2. The CISO will review password/passphrase exceptions periodically.
3. IT will consider password/passphrase requirements when evaluating new or replacing existing non-compliant systems.

IV. DEFINITIONS

A. "**Information Resources"** means information owned or possessed by the University, or related to the business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information.

B. "Passphrase or Password" means a string of words that must be used to gain access to a computer system or service.

C. "MFA (multifactor authentication)" means using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Revision Effective Date	**Purpose**