UNIVERSITY of NORTHERN COLORADO

Requirements and Guidance for Passphrase Management (Excerpt for Web)

Password Policies:

1. Complexity Requirements
    - All passphrases (passwords) must contain at least 3 of 4 complexity categories:
        - Uppercase letter
        - Lowercase letter
        - Number 0-9
        - Special character (~!%^&*_-+=|\(){}[]:;"'<>,.?/)

2. Access to all *Private* or *Restricted* resources must be secured with multifactor authentication.

3. All passwords to a PCI system or a system that touches a PCI environment must adhere to the following standards:

    - The passwords on these systems should be at least 16+ characters but at minimum of 12 characters. This is only permitted in cases where there is a technical issue that prevents a 16+ character password.
    - These passwords must be set to expire within 180 days. The password must be different from the previous 6 passwords.
    - Multifactor authentication must be used for authentication to these systems.

4. *Restricted* systems must be secured with at least 16+ characters, preferably 32+ characters.

5. The minimum password length for any system containing UNC *Private Data* must be at least 12+ characters.

6. Account passwords must be unique for each account. For example: you cannot use the same password for both your first.last and your student account.

7. If for any reason the above policy cannot be followed an exception needs to be filed with the security team. IT.Security@unco.edu

- **Do not share your passphrase with anyone for any reason.**

  Passphrases should not be shared with anyone, including any other students, faculty, or staff. In situations where someone requires access to another individual's protected resources the resources in question can be shared by granting permissions to the resource though a UNC business process. For example, Microsoft Exchange calendar will allow a user to delegate control of his or her calendar to another user without sharing any passphrases. Passphrases should not be shared even for the purpose of computer repair.

- **Change your passphrase periodically**.

  As a rule, changing your passphrase every 90 days is recommended. However, you may choose to vary the frequency of passphrase changes based on the privilege or access level of the account. If you suspect someone has compromised your account, change your passphrase immediately.

- **Do not write your passphrase down or store it in an insecure manner.**

  As a rule, you should not write down your passphrase. In cases where it is necessary to write down a passphrase, that passphrase should be stored in a secure location and properly destroyed when no longer needed (see Guidelines for Data Protection).

- **Do not use the same passphrase for multiple accounts.**

  While using the same passphrase for multiple accounts makes it easier to remember your passphrases, it can also allow an attacker to gain unauthorized access to multiple systems by compromising your passphrase from a different account.

Revision History

Version	**Published** YYYY/MM/DD	**Author**	**Description**
1.0	2015/02/10	Matt Langford	Original publication.
1.1	2016/05/04	Matt Langford	Establish links
1.2	2017/07/20	Matt Langford	Annual review. Update links.
1.3	2019/05/23	Matt Langford	Annual review.
1.4	2020/08/12	Matt Langford	Annual review, updated links, minor content changes.
1.5	2022/12/19	Matt Langford	Annual review
1.6	2023/06/02	Matt Langford	Updating so this covers all password policies