UNIVERSITY of NORTHERN COLORADO

# IM&T Internal Password Policy for University of Northern Colorado

## Purpose:

This document outlines the password policy for the IM&T department to include accounts for computers, servers, appliances, databases, and any other credential that the IM&T department owns, manages or uses.

## Definitions:

*PCI systems* – Any computer, server, service, database, etc. that touches an environment where credit card data is processed or passed in transit. Or any credential that could be used to access such a system. **UNC does not store credit card data electronically.**

*Restricted systems* – Any computer, server, service, database, etc. that is critical to IM&T or university infrastructure. Any system, as mentioned above, that can affect life, safety, or any other systems deemed Restricted as outlined in the data classification document.

*Private systems* – Any computer, server, service, database, etc. that contains PII data, data that are proprietary to the university or individuals within the university, research, or is otherwise deemed private as per the data classification document.

## Password Policy:

1. All .ad or .admin account passwords must have at least 16+ characters and must include at least one upper and lower case alpha character, at least one number, and at least one special character.

2. 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 and must include at least one upper and lower case alpha character, at least one number, and at least one special character.
    - A minimum of 12+ characters and must include at least one upper and lower case alpha character, at least one number, and at least one special character and is acceptable only in cases where there is a technical issue that prevents a 16+ character password.
    - These passwords must be set to expire within 90 days. The password must be different from the previous 6 passwords.

   - Two factor authentication should be used as a second line of authentication for these systems.
   - In the case of remote access two factor authentication is a requirement.

3. Private or Restricted systems must be secured with at least 16+ characters preferably 32+ characters and must include at least one upper and lower case alpha character, at least one number, and at least one special character.

4. The minimum password length and complexity is to be at least 12+ characters and must include at least one upper and lower case alpha character, at least one number, and at least one special character. This password will be good for only 90 days and should only be used if a technical issue prevents the use of 16+ character passwords.

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

6. If for any reason the above policy cannot be followed an exception needs to be filed with the security team.

The following are the specific password guidelines to be followed:

Minimum Standard only to be used if a technical issue prevents the use of a stronger password.

- 12+ characters (upper and lower alpha) 1+ numeric and 90 days to expire
- 12+ characters (upper and lower alpha) 1+ numeric and 1+ special character 180 days to expire

Acceptable for all systems.

- 16+ characters (upper and lower alpha) 1+ numeric and 1+ special characters 270 days to expire

Preferred length for any Restricted systems or service accounts.

- 32+ characters 1095 days to expire

In all instances passwords history shall retain the previous 6 passwords which cannot be reused.

IM&T employees should use the strongest password standard possible.

## Revision History

| Version | Published | Author | Description |
|---|---|---|---|
| 1.0 | 2015/12/09 | Matt Langford | Original draft |
| 1.1 | 2015/01/23 | Matt Langford | Update |
| 1.2 | 2015/05/27 | Matt Langford | Updated expiration days |
| 1.3 | 2016/08/17 | Matt Langford | Annual review. Made improvements to the text that did not impact the content. |
| 1.4 | 2017/07/20 | Matt Langford | Annual review. Minor revisions. |
| 1.5 | 2018/06/05 | Matt Langford | Annual review. Template update |
| 1.6 | 2019/05/23 | Matt Langford | Annual review. |