



IT Account and Access Procedure

Revision History

Version	Date	Editor	Nature of Change
1.0	3/23/06	Kelly Matt	Initial Release

Table of Contents

1.0 Overview.....	1
2.0 Purpose.....	1
3.0 Scope.....	1
4.0 Passwords.....	1
4.1 User Requirements.....	1
4.2 Technical Requirements.....	1
4.3 Procedural Requirements.....	2
4.4 Bad Password Practices:	2
4.5 Password Self Service.....	3
5.0 Account Management	3
5.1 Account Taxonomy.....	3
5.2 Granting Access	3
5.3 Administrative Accounts:	3
5.3.1 Administrative Account Password Requirements:	4
5.3.2 Two-factor authentication for Administrative Account: Error! Bookmark not defined.	
5.4 Temporary Privilege Accounts:	4
5.5 Reevaluation of System Access	4
5.6 Revoking Access.....	4
6.0 Enforcement.....	4
7.0 Related Policies, Procedures, and Codes of Conduct.	4
Appendix A: Active Directory Password Configuration	5
Appendix B: IT Account and Access Procedure Exception	6

1.0 Overview

All individuals who access the University of Northern Colorado's computing infrastructure have a responsibility to safeguard these systems and data. User accounts and passwords are two mechanisms through which this is accomplished. This procedure establishes the rules by which user accounts and passwords should be managed and used on any computing resource belonging to the University.

2.0 Purpose

The ability to access information and/or application systems within UNC's computing environment must be based on clearly defined business requirements. This document aids in establishing clear definition for account and password management.

3.0 Scope

This Procedure applies to employees, contractors, consultants, temporary employees, and other workers at UNC including all personnel affiliated with third parties. This Regulation applies to all equipment that is owned or leased by UNC.

4.0 Passwords

Passwords are an important form of protection used to ensure that the University's information is stored and processed in a secure manner. Due to this, passwords must be defined and implemented in accordance with a minimum set of standards. This section establishes the rules by which password should be assigned and used on any computing resource belonging to the University

4.1 User Requirements

- Users are responsible for all activity performed with their individual user-ID. User-IDs may not be utilized by anyone the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users must not perform any activity with IDs belonging to other users.
- Users must choose their own passwords. They should not be easily guessed but easy enough for the user to remember without writing it down.
- Users are responsible for maintaining the security of their passwords.
- Passwords should NEVER be shared, written down, or stored electronically. If a user must write a password down, it should never be written on something that can be associated with the user (i.e. business cards). If passwords need to be stored electronically an encryption schema that is approved by the Office of Information Security must be used. (See Appendix B IT Account and Access Procedure Exception)
- The sharing of a single user ID or associated password among several users is prohibited
- Prior to receiving an account, all users must sign a statement acknowledging that they have received and reviewed the university's IT acceptable user regulation.
- Access to various types of information may be blocked. Individuals will be required to obtain appropriate approval prior to being allowed access. Individuals accessing university data without a valid business need may be subject to disciplinary action.
- If a user believes their password has been compromised, the user should contact the UNC Technical Support Center immediately for assistance.

4.2 Technical Requirements

- Personal computers shall have a screen saver password set to automatically engage after 10 minutes of inactivity.
- Where technically feasible all systems will at a minimum prompt for user ID and employ passwords for account access.
- All accounts must be disabled after 5 unsuccessful logon attempts.
- Where technically feasible password complexity must be programmatically enforced.
- Passwords must be a minimum of 9 characters long for all user accounts.

- Passwords should not be displayed in plain text on the monitor when entered.
- Where technically feasible single-sign-on technology should be used.
- Passwords must contain characters from at least three of the following four classes:
 - Upper case letters
 - Lower case letters
 - Numeric (0 to9), this should not be the first or last character
 - One special character, this should not be the first or last character
- Where technically feasible a password history of 14 passwords must be retained to limit password reuse.
- Where technically feasible the minimum password age shall be 1 day.
- User accounts must change passwords every 90 days.
- Users must be able to change their own password independent of any external party.

4.3 Procedural Requirements

- Administrative accounts must follow the procedures identified in section 5.2.1.
- TSC personnel must verify the identity of a user prior to resetting the password. Identity verification may be done by using voicemail call back or by some other approved form of identity verification.
- A system administrator must manually unlock accounts.
- New accounts or accounts for which a password has been reset must be set to expire at the next login attempt.
- Passwords must not be embedded in scripts or application code and will not be used in URL passing.
- For internet application, separate the delivery of user ID and passwords is required.
- All new or reset passwords must meet complexity rules and be randomly generated. No common or default passwords will be used.
- No default system and application passwords are allowed.
- Passwords exempted from regular changing must have an approved exception. Exceptions must be approved by the Office of Information Security and the appropriate director for the respective IT unit. The password will be a minimum of 12 characters (or the maximum permitted by technology, whichever is less) in length. Upon renewal of the exception, the password must be changed.
- User accounts with non-expiring passwords are prohibited.

4.4 Bad Password Practices:

The following are some examples of practices and behaviors that can result in weak or bad passwords. Under no circumstances should individuals use passwords that utilize the following:

- Passwords that match the account ID
- Passwords that contain the user account owner's name, first middle or last.
- Passwords that contain the users bear ID or Social Security number
- Any vendor or product name
- Any consecutive or repeating keyboard characters e.g. "123", "jkl"

Individuals are strongly urged to not use the following when creating there passwords:

- The name of a food, celebrity, sport or sports team
- IT Account and Access Procedure
- Words that are found in common dictionaries English or otherwise
- Using sequential passwords
- Passwords that contain family member or pet names

4.5 Password Self Service

Password Self Service is a powerful and very useful tool. This technology can reduce support costs and significantly reduce support calls. The benefits from these tools are significant. However, due to the very powerful nature of these tools precautions must be in place to guard against misuse and abuse. The following are base level guidelines that a password self service solution must meet.

- Servers and systems used to provide password reset activities must be sufficiently secured and have limited well defined access rights.
- All password reset related activities must be handled via an encrypted channel
- At no point in the password reset process should any data used to reset passwords be passed in clear text.
- Information gathered and used to perform password resets must be sufficiently unique to the given individual.
- Information that a large number of individuals may have in common should not be used to reset user passwords.
- Information gathered and used to perform password resets must not be easily guessed or easily obtained. Examples include but are not limited to the following:
 - Mothers maiden name
 - Data of birth
 - Place of birth
 - Favorite Color

5.0 Account Management

User accounts are the primary form of digital identity and access to UNC computing resources. As such, it is vitally important that these digital identities be managed in a consistent fashion. The following outlines account management practices for the University of Northern Colorado.

5.1 Account Taxonomy

The following naming standards will be used for all accounts created within the universities computing environment.

- User accounts: first name.last name
- Administrator accounts: last.admin
- Service accounts: unique description.service (In addition to a standard descriptions a primary contact must be defined and documented in a description or comments field for the account. The primary contact should be defined by position as well as name.)

5.2 Granting Access

Network access must be granted based on business requirements. Privileges will be granted only when there is a legitimate need.

- User accounts require proper authorization prior to being established.
- To maintain individual accountability and system integrity, user IDs must be unique within and across computing platforms.
- Each computer and communication system user-ID must uniquely identify only one user. Shared or group user-IDs are permitted only when the use of a unique user-ID is not feasible. Exceptions must be documented and approved by management and the Office of Information Security.

5.3 Administrative Accounts:

Each request for administrative rights will be made in writing and will include the following:

- Justification for the need for the account
- Line management approval

- Information Security Office approval
- IT Management approval

5.3.1 Administrative Account Password Requirements:

Accounts that have elevated privileges must adhere to the following password requirements:

- All administrative, technical support accounts, and accounts deemed to have privileged access must change their password every 45 days.
- These accounts, where technically feasible, must make use of a 14 character password.
- Password, where technically feasible, must consist of uppercase, lowercase, numbers, special characters, and extended ASCII characters.

5.4 Temporary Privilege Accounts:

Temporary privilege accounts will be re-evaluated every 6 months. Temporary privilege accounts will only be issued at the discretion of the UNC Information Security Office with the approval of IT management. Duration of such accounts will be negotiated based upon the business need and only when there is no viable alternative solution. These accounts will be limited in function, allowed only to perform the required task/s.

Projects:

When privileges are granted for a particular project, these privileges will be revoked at the completion of the project.

5.5 Reevaluation of System Access

System privileges should be reviewed on a periodic basis. Account and privileges that no longer appropriate must be promptly revoked.

- All user accounts that have been inactive for 60 consecutive days will be reviewed, disabled, and deleted from the system as necessary.
- New accounts not activated within 14 days must be disabled.

5.6 Revoking Access

The following guidelines specify the requirements for separation of employees and contractors.

- User account shall be immediately disabled upon separation from the university.
- As part of the separation Human Resources will submit a request to the TSC to have the account disabled.
- Reactivating an account that has been disabled will require the user to follow the initial request process.

6.0 Enforcement

Those found to have violated this regulation may be subject to suspension of computer access privileges.

7.0 Related Policies, Procedures, and Codes of Conduct.

All applicable laws and University policies, regulations and procedures bind UNC students and employees.

- UNC Acceptable Use Regulation:

Appendix A: Active Directory Password Configuration

Active Directory Password Policy Setting:

Policy	Setting
Enforce password history	14 passwords remembered
Maximum password age	90 days
Minimum password age	1day
Minimum password length	9 characters
Password must meet complexity requirements	Enable
Store passwords using reversible encryption	Disabled

Account Lockout Settings:

Policy	Setting
Account lockout duration	lockout until unlocked by admin
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Appendix B: IT Account and Access Procedure Exception

IT Account and Access Procedures exception can only be granted after a security review and with applicable functional area director approval. Exceptions will only be granted in cases where there is a well justified need and business case for not adhering to IT Security Procedures.

Mitigating controls will be required in any case were an exception to this procedure is granted. These controls must be approved by the Office of Information Security and documented in this form.

Exceptions are granted for a maximum of 12 months but can be granted for intervals shorter than 12 months. Upon expiration of an exception a review will be conducted with the requester and the validity of the exception examined. If the exception is still deemed necessary and prudent the requester must submit a new exception form for the new time period.

Passwords for the account must be changed at the expiration of any given exception.

Requester:
Position:
Department:

Account Name:

Technical Reason for Exception:

Business Justification:

Security Requirements and Mitigating Controls:

Security Approval
Print Name:
Sign:

Date:

Unit Director Approval:
Print Name:
Sign:

Date:

Exception Termination (Max 12 Months): _____