THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Issuing Office(s)
Information Technology Services

Responsible University Officer(s)
Chief Information Security Officer

UNIVERSITY STANDARD

Title

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL STANDARD ON PASSWORDS FOR GENERAL USER, ADMINISTRATOR, AND SYSTEM ACCOUNTS

Introduction

PURPOSE

This document sets forth password requirements for all UNC-Chapel Hill individual user accounts, administrator accounts, and system accounts. All passwords used to access computing systems that connect to the University network or contain University data must meet the specific minimum password requirements described below and must be under the control of individual users. Any suspected compromise of a password must be reported immediately.

This standard sets minimum requirements. Group, unit, or departmental standards, specific system security requirements, may impose more stringent or additional requirements than the minimum requirements set forth herein. Best practice guidance may exceed these minimum requirements.

SCOPE OF APPLICABILITY

Any faculty member, staff member, student, temporary employee, retiree or other affiliate, contractor, outside vendor, or visitor to campus ("User") who has access to UNC-Chapel Hill owned or managed information or the UNC-Chapel Hill network through computing devices owned or managed through UNC-Chapel Hill or through permission granted by UNC-Chapel Hill.

Standard

GENERAL REQUIREMENTS

The general requirements represent minimum standards applicable to general user, administrator, and system accounts. NOTE: These standards must be met even if a system does not enforce them with technical controls (users must select passwords meeting or exceeding these standards even when a system would allow a weaker password). University business/academic units or specific systems may require passwords exceeding these minimum standards. Users are encouraged to use strong passwords above and beyond these minimum requirements. These standards reflect baseline expectations for all University systems, users, and accounts. (Administrator and system accounts have exceptions and additional requirements described below.)

Passwords will:

- be at least eight characters long.
- contain at least one upper-case letter, at least one lower-case letter and at least one numerical digit
- contain at least one of these characters: !@#$%&*+={}?<>'"
- not start with a hyphen, end with a backslash (\), or contain a double-quote (") anywhere except as the last character.

Password Sharing:

All passwords are to be treated as confidential sensitive information. Passwords will not be shared with others except in emergency situations (see “System Accounts” and “Exceptions” below for special cases). In emergency situations, a password may be shared with a supervisor but must be changed immediately once there is no longer an emergency need. Examples of unauthorized sharing include sharing passwords with administrative assistants, coworkers or spouses. If you need assistance with how to share your email correspondence with an administrative assistant or coworker -- without sharing your password -- please visit help.unc.edu

General Password Rules:

- Users shall only use account credentials for which they have been authorized.
- All Users are responsible for maintaining the security of their passwords. In the event that an account is believed to have been compromised, the person detecting the incident should report the incident immediately to 919-962-HELP and the Helpdesk should be asked to open a critical ticket. In addition, the responsible system administrator should be contacted directly and informed about the password compromise. An account is deemed compromised if it is known or reasonably suspected of being used by an unauthorized party. A compromise will affect the functionality of any account, and the account will not be restored until the risk associated with any such compromise has been mitigated.
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset upon installation of the affected application, device, or operating system.
- Use of standard user accounts to run system services is prohibited.
- Users may not attempt to “crack” (decrypt) encrypted or hashed passwords without the explicit written permission of the Information Security Office.
- A password may not have been used within the last 12 months.
- A password and Onyen or other user ID shall share fewer than six (or, if shorter, the length of the user ID) consecutive common characters.
- A password shall not include personal information, such as Social Security number, name or date of birth.
- A password should avoid single words found in any English or foreign language dictionary (multiple words are acceptable/encouraged.)
- Passwords expire within 91 days and each User is required to reset them before expiration.

ADMINISTRATOR ACCOUNTS

In addition to all general requirements for account passwords described above, users with system or application administrator roles (including privileges permitting the use of a program such as “sudo,” Allowing a user to perform superuser/administrator commands) must also adhere to a more rigorous standard for password management,

as set forth below including use of good judgment. The following requirements for accounts with administrator privileges (see below for "system" or "service" accounts):

- A user account that has system level ("administrator") privileges or programs such as "root" access shall have a different password from personal accounts or other accounts not protected by two-factor authentication, known by that user. System or application administrators who use their Onyen in their administrator roles must follow the guidance below regarding administrator accounts.
- Administrator Accounts must meet one of the following combinations of controls:

2-Step verification	Password Length (minimum)	Password change duration (maximum)
No	15 characters	91 days
Yes	8 characters	91 days
Yes	15 characters	365 days

NOTE: If the same password is in use on multiple systems (as with use of an Onyen for authentication) then 2-Step Verification must be in use on every account the user has administrative privileges with that password in order to reduce the password length or increase its duration above the non-2-Step requirement.

NOTE: Systems may not support longer-duration passwords, this option is allowed where it is technically feasible.

- If an employee has dual roles as user and administrator, whenever possible, the employee should log into the account with the least privileges to perform their work.
- As an exception to any password expiration rules, a password on an administrator account must be changed whenever the administrator responsible for the account leaves the organization or changes roles.
- Systems must be configured to log all log-in attempts (successful and unsuccessful). Where technically feasible, logging should be configured to include UNC-Chapel Hill system name, system account name, remote computer information such as IP address or remote computer name, and relevant time and date information. Logs must be retained according to the requirements of the Information Security Controls Standard.

SYSTEM ACCOUNTS

System accounts (also known as Service or Device accounts) are typically not associated with an individual user. These accounts may be managed by more than one individual (an exception to the password-sharing prohibition). These accounts are used to run IT services for applications (e.g., web services, database services) or as built-in accounts in an operating system or application such as “root” or “system.”

In addition to the requirements above, the password length and complexity requirements should be increased to increase safety and to allow for less frequent password expiration that may be appropriate to ensure that key services are not disrupted due to password expiration.

- Service accounts specifically created for services/applications must only be used for system services. Use of a standard user account to run system services is prohibited. End users and administrators are not allowed to remotely log in using service account credentials except as needed in the scope of supporting the specific service. Systems/devices should be configured to prevent remote logins to service accounts wherever technically feasible.

The following password standards apply to service accounts:

- Password Expiration: 365 days
- Minimum Password Length: 15 characters
- Lock-out Period: N/A
- Renewed Log-in Required: N/A

Examples of service accounts:

- Web service account created and used to run a web service
- A database account created to run a database service
- An application account created to run a specific application

Password Management Software: Password management software may be used as long as it employs AES128 bit encryption or stronger, leverages greater than TLS version 1.0 for encryption in transit and follows the other guidance in this document.

EXCEPTIONS

Specialty Devices: Due to the wide variety of specialty devices and their frequently limited capabilities, particularly with regard to password management, specialty devices such as fax machines, printers, physical access control equipment, copy machines, specialty lab equipment, phones, etc., are not subject to this standard *unless* those devices are used to store or protect sensitive information or perform mission-critical functions. Where appropriate, departments should develop their own specific standard for the specialized devices they use to ensure that adequate authentication controls are present.

Departments may employ more stringent password standards than those outlined in this document, but not less stringent than those listed here.

Definitions

Administrator: User account with higher privileges than a standard user of an application or operating system. This includes administrators of servers, multi-user applications, privileged access to applications, or sudo access. A user who can set privilege levels for other users is an administrator. NOTE: This does not include common use of "local-admin" privileges on individual devices.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges.

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Password: A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.

Unauthorized Access: Occurs when a user, legitimate or unauthorized, accesses resources that the user is not permitted to use.

Sensitive Information: Information classified as Tier 2 or Tier 3 in the UNC-Chapel Hill Information Classification Standard.

Related Requirements

EXTERNAL REGULATIONS AND CONSEQUENCES

Failure to comply with this standard may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this standard may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with UNC-Chapel Hill.

Violation of this standard may also carry the risk of civil or criminal penalties.

UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES

Password Policy for General Users
Password Policy for System and Application Administrators
Information Classification Standard
Acceptable Use Policy
UNC-Chapel Hill Onyen Password page
UNC guidelines for creating a strong password
UNC Help & Support: What is Sensitive Information,
UNC Help & Support: Securing Sensitive Information
UNC Help & Support: Examples of Sensitive Information.

Contact Information

PRIMARY CONTACT(S)

1. ITS Information Security Office
   Title: Information Security Office
   Unit: ITS
   Email: help.unc.edu
   Phone:919-962-HELP

OTHER CONTACTS

ITS Policy Office its_policy@unc.edu

To report a compromised password, please call 919-962-HELP.

Important Dates

- Effective Date and title of Approver: (Previous documents, UNC-Chapel Hill Password Standard for General Users and Password Standard for System and Application Administrators)
    a. Effective Date: 3/16/2015 (both)
    b. Approver: Chief Information Security Officer

- Revision and Review Dates, Change notes, title of Reviewer or Approver:
    a. Last Revised Date: 10/25/2017
    b. Revised by: Chief Information Security Officer
    c. Substantive Revisions: Revised password complexity requirements. Combined User and Administrator Standards into single document. Removing section on RACF. Removed timeout control to Information Security Controls Standard. Provided options for password duration involving 2-factor Verification. Clarifications throughout.