UNC INFORMATION TECHNOLOGY SERVICES

Responsible UNC ITS Officer
Chief Information Security Officer

Responsible Office
Information Technology Services

UNC-Chapel Hill Password Standard for General Users

Purpose of this Standard

This document sets forth password requirements for all UNC-Chapel Hill individual user accounts. All passwords used to access computing devices that connect to the University network must meet the specific minimum password requirements described below and must be traceable to individual users. Any suspected compromise of a password must be reported immediately.

This standard does not supersede any unit or departmental password standard that imposes more stringent requirements for general users than the minimum requirements set forth herein.

Audience

Any faculty member, staff member, student, temporary employee, 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

Passwords will:

- be at least eight characters long.
- contain at least one 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. 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 see http://help.unc.edu/5989.

General Password Rules:

- Users will only use account credentials for which they have been authorized.
- 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 will never be inserted into plain text emails, stored unencrypted in computer files, or written down.
- A password may not have been used within the last 12 months.
- A password and Onyen or other user ID will share fewer than six (or, if shorter, the length of the user ID) consecutive common characters.
- A password will not include personal information, such as Social Security number, name or date of birth.
- A password should avoid words found in any English or foreign language dictionary.
- 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 that the account is 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.
- Passwords expire within 91 days and each user is required to reset them before expiration.

Lock-Out:

After 10 failed attempts to log-in, the system will lock-out a user for 30 minutes. After 30 minutes, users may attempt to log in again. Each system will be locked out automatically after 30 minutes of inactivity.

Compliance

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.

Roles and Responsibilities

Users shall comply with the UNC-Chapel Hill password standards listed in this document.

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

Definitions

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.

Password Circulation: An attempt to bypass the basic password requirement that prohibits reusing the same password within a specified period of time by changing the password repeatedly within a brief period of time in order to be able to reuse the password earlier than intended.

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

Sensitive Information: is defined as information that is protected against unwarranted disclosure.

Related Documents

UNC-Chapel Hill Onyen Password page
UNC guidelines for creating a strong password
Password Policy for System and Application Administrators

Contacts

Subject	Contact	Telephone	Online/Email
Standard Questions	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
Request Information Security Consulting	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
Report a Violation	UNC ITS Information Security Office	919-962-HELP	N/A

Information Resources

See: UNC Help & Support: What is Sensitive Information, UNC Help & Support: Securing Sensitive Information and UNC Help & Support: Examples of Sensitive Information.

Document History

- Effective Date and title of Approver: 3/16/2015 Chief Information Security Officer
- Revision and Review Dates, Change notes, title of Reviewer or Approver: Revision 11/10/2015, Changed from 90 to 91d expiration to alter pattern of weekend expirations, Chief Information Security Officer