UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

UNC-Chapel Hill Password Policy for General Users

Policy Statement

All UNC-Chapel Hill individual user accounts are required to use a password in accordance with the University Information Technology Services (ITS) password standard. All passwords used to access computing devices that connect to the UNC-Chapel Hill network must meet the specific minimum password requirements described within the password standard and must be traceable to individual users. Any suspected compromise of a password must be reported immediately.

This policy does not supersede any unit or departmental password policy 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.

Reason for Policy

A growing number of information security incidents result from unauthorized access to information stored on computers. Frequently, access to such information is controlled through the use of password authentication.

The failure to protect information through the use of strong passwords that satisfy the requirements set forth in this document may result in incidents that expose sensitive information and/or impact mission-critical UNC-Chapel Hill services. Adherence to this policy is essential to ensure the security of UNC-Chapel Hill information.

Compliance

Failure to adhere to these password policies 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 policy may be referred to the UNC-

Chapel Hill Office of Student Conduct. Contractors and vendors who fail to adhere to this policy may face termination of their business relationships with UNC-Chapel Hill.

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

Roles and Responsibilities

Users shall comply with the University password policies listed in this document.

Departments may employ more stringent password policies 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 by the policy.

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

Sensitive Information: is defined as information that is protected against unwarranted disclosure. See: UNC Help & Support: What is Sensitive Information, UNC Help & Support: Securing Sensitive Information and UNC Help & Support: Examples of Sensitive Information.

UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Related Documents

Standard on Passwords for General User, Administrator, and System Accounts
UNC-Chapel Hill Onyen Password page
UNC guidelines for creating a strong password
Password Policy for System and Application Administrators
Definition of Sensitive Information

Contacts

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

Document History:

Last Revision: March 12, 2015