UNC INFORMATION TECHNOLOGY SERVICES

Responsible UNC ITS Officer
Chief Information Security Officer

Responsible Office
Information Technology Services

UNC-Chapel Hill Password Standard for System and Application Administrators

Purpose of this Standard

This document sets forth password requirements for all system and application administrators. All passwords used to access computing devices that connect to the University network must meet the specific minimum password requirements described below. 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 system and application administrators than the minimum requirements set forth herein.

Audience

All employees formally fulfilling the duties of System or Application Administrators.

Standard

- A user account that has system level ("administrator") privileges or programs such as "root" access shall have a different password from all other accounts known by that user.
- A user account that has system level ("administrator") privileges or programs such as "root" access must have its password expiration period set to 30 days or the user of such an account may use two-factor authentication as an alternative.
- 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 the 30-day password expiration, 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 for a minimum of 90 days or up to 250 MB of storage space.

Standards for Special Accounts, Specialty Devices, and Password Management Software

Service Accounts: Service accounts are system/device accounts used to run IT services for applications (e.g., web services, database services). The password length and complexity requirements are increased 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
- A password must contain at least one letter and at least one numerical digit.
- A password must contain at least one of these characters: !@#$%&*+={}?<>"'
- A password must not: start with a hyphen, end with a backslash (\), or contain a double-quote (") anywhere except as the last character.

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

Resource Access Control Facility (RACF) Accounts: Due to special technical limitations, RACF accounts may not fully conform to some of the requirements listed in this password standard. RACF accounts must be configured to meet this standard to the greatest extent possible and as far as Technically Feasible. The Information Security Office (ISO) should be notified in writing about requirements that are not technically feasible to meet.

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.

Password Management Software: Passwords may not be written down or stored in clear text, although password management software may be used as long as it employs AES128 encryption or stronger. The password used to access this application must meet the requirements set forth in this standard.

Compliance

Failure to adhere to these password standards 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 and vendors who fail to adhere to this standard may face termination of their business relationships with the University.

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

Roles and Responsibilities

System and Application Administrators: Ensure password standards outlined in this standard are met and maintained and the University's Policy for General Users is followed.

Definitions

Administrator (System or Application): Generally, a staff member that manages and maintains computer devices for the University and is authorized to have access beyond that of an end user.

Technically Feasible: Technically possible and does not materially impact the ability of the technology or user to complete mission-critical tasks.

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

Document History:
Created: March 13, 2015