UNC
INFORMATION
TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Password Policy for System and Application Administrators

Policy Statement

In addition to the rules described in the University's Password Policy for General Users, all System and Application Administrators must adhere to the password rules listed in this policy. These specific password standards must be enforced as much as technically feasible. The requirements in this policy apply to all administrator-level passwords on UNC-Chapel Hill owned or managed computing devices that connect to the University network.

This policy does not prevent any unit or department from creating a separate password policy as long as, at a minimum, all requirements specified in this Policy and in the Password Policy for General Users are met.

Scope

This policy sets forth password requirements for System and Application Administrator accounts.

Audience

This policy applies to all employees formally fulfilling the duties of System or Application Administrators.

Compliance

Failure to adhere to this policy may result in disciplinary actions against the respective employee, up to and including termination of employment. Violation of this policy can, in some cases, also carry the risk of civil or criminal penalties.

If, for technical reasons, the available standards cannot be enforced, the System or Application Administrator must inform the Information Security Office (ISO) in writing about any devices that do not meet the majority of the standards. Information that must be provided includes: IP address of the device, system location, user name, administrator name, and standards not enforced.

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: Where it is determined that it is feasible to implement in a manner that is technically possible and does not materially impact the ability of the technology or user to complete the task.

Reason for Policy

Due to the amount and potential sensitivity of data controlled by System and Application Administrators, passwords for administrator accounts are subject to additional rules beyond those set forth in the University's Password Policy for General Users.

The failure to protect data through the use of strong passwords for administrator accounts can result in incidents likely to expose the University's Sensitive Information and/or impact Mission-Critical University services (See Password Policy for General Users for the definition of these terms).

General Standards

- 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 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:

Service Accounts	
Password expiration	365 days
Minimum length	15 characters
Lock-out period	Not applicable
Renewed log in required	Not applicable

- **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 policy. RACF accounts must be configured to meet this policy 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 policy *unless* those devices are used to store or protect Sensitive Information or perform Mission-Critical functions. Where appropriate, departments should develop their own specific policies 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 policy.

Related Documents

UNC-Chapel Hill Onyen Password page
Password Policy for General Users
Help-document on selecting a strong and effective password

Contacts

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Subject	Contact	Telephone	FAX
Policy Questions	The University’s Information Security Office	919-445-9393	919-445-9488
Report a Violation			
Request Information Security Consulting			

History

Effective Date:

Revised Date: **6/30/10**

Next Review Date: