UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

UNC-Chapel Hill 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 UNC-Chapel Hill's Password Standard for System and Application Administrators. The requirements in this policy apply to all administrator-level passwords on UNC-Chapel Hill owned or managed computing devices that connect to the UNC-Chapel Hill network.

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

Audience

This policy applies to all employees formally fulfilling the duties of system or application administrators. This policy also applies to contractors, vendors and others managing UNC-Chapel Hill systems.

Reason for Policy

Due to the sensitivity of information 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 information through the use of strong passwords for administrator accounts can result in incidents likely to expose UNC-Chapel Hill's sensitive information and/or impact mission-critical University services (See Password Policy for General Users for the definition of these terms).

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.

Contractors and vendors who fail to adhere to this Policy may face termination of their business relationships with the University.

If, for technical reasons, the policy 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 policy so that compensating controls can be explored.

Roles and Responsibilities

System and application administrators: Ensure password policies outlined in this document and the University's Policy for General Users are met and maintained.

Definitions

Administrator (System or Application): Generally, a staff member who manages and maintains computer devices for UNC-Chapel Hill 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
Password Policy for General Users
Help-document on selecting a strong and effective password
Password Standard for System and Application Administrators

Contacts

Subject	Contact	Telephone	Online/Email
Policy 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:
Last Revised: March 12, 2015