University of North Carolina General Administration
Information Resources Division (UNC-GA IR)

General Password Security Guidelines

This document outlines the guidelines and practices for the creation and protection of passwords for the University of North Carolina General Administration IT resources. Good password practices are an important component in protecting UNC-GA IT resources. It is the responsibility of the user to take the appropriate steps in creating, maintaining and protecting their passwords.

These guidelines shall apply to all employees ("users") of UNC General Administration who use or access UNC-GA IT resources. "Users" also include subcontractors, visitors, interns, or other persons who have reason to access UNC-GA IT resources.

General Password Security

Passwords should be managed according to the following standards and guidelines. Applications/system software should be configured to enforce these standards and guidelines whenever possible.

Passwords should:

- be changed on a regular basis. (The default UNC-GA requirement on frequency of change is 90 days),
- be a minimum of 8 characters and contain at least 1 number and 1 symbol,
- be case sensitive and the use of dictionary words or proper names within passwords should be avoided,
- never be saved or "remembered" when prompted by an application,
- always be entered in a non-display field ,
- be changed whenever there is evidence of a possible or actual intrusion to the respective user account or system,
- never be given out or shared with other users and users should never be asked to reveal passwords,
- never be written down or recorded in any way that would allow unprotected access by any non-owner of that password, and
- be encrypted when transmitted over a network.

Default/initial passwords should always be changed immediately following the initial login and passwords should not be repeated for at least 270 days (3 x 90 days).

User accounts should be disabled or locked after 3 consecutive unsuccessful login attempts within a 15 minute period. The lockout time should be set at a minimum of 30 minutes.