GEORGIA
DEPARTMENT OF NATURAL RESOURCES

Password Control Standards

The Georgia Department of Natural Resources requires the use of strictly controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II).

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for Accessing PHI, CI, and II:

Users are responsible for complying with the following password standards:

- Passwords must never be shared with another person, unless the person is a designated security manager.
- Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed).
- Passwords must be constructed with the following characteristics:
    - Are at least eight characters in length
    - Must contain characters from at least three of the following four types of characters:
        - English upper case (A-Z)
        - English lower case (a-z)
        - Numbers (0-9)
        - Non-alpha special characters ($, !, %, ^, ?)
    - Must not contain the user's name or part of the user's name
    - Must not contain easily accessible or guessable personal information about the user or user's family. (such as birthdays, children's names, addresses, etc…)
- Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
- Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
- When creating a password, <u>do not</u> use words that can be found in dictionaries or words that are easily guessed due to their association with the user (children's names, pets' names, birthdays, etc.). A combination of alpha and numeric characters is more difficult to guess.