Best Practice Guidelines for General HSEN Passwords and PCs

Passwords

Setting Up a Password

- Initially, each account is assigned a password. After the user has successfully dialed into the HSEN network, the users' password must be changed.
- To ensure the security and integrity of the network, each user is provided with a user account to access network resources.

In the HSEN domain, each user's password must meet the following complexity requirements:

- Password cannot contain all or part of the user's account name.
- Password must be at least eight characters in length, not to exceed 13.

Out of the next four categories, passwords must consist of three of the following:

- Alpha uppercase characters (A through Z)
- Alpha lowercase characters (a through z)
- Numeric characters (0 through 9)
- Non-numeric characters (!, $, #, %, etc.)

Examples of complex passwords include:

- A strong password could include the first letters of a familiar phrase with additional special characters and numbers inserted where the user will remember. Ex: Every good boy does fine 2, 3, * equaling Egbdf23*or Tis the season to be jolly which could be Tt$tbj12 ($ for S and12 for twelfth month). Other examples that are not as complex include:
- Apricot$
- ,January1
- !Purplecrayon

Other facts about your HSEN accounts:

- The maximum age of a password is 90 days. Fourteen days prior to expiration, you will be prompted to change your password.
- You have 6 valid attempts to sign on to the network before your account is locked out.

- You cannot reuse your last 13 passwords.
- Password age is one day; therefore, you can only have your password changed once per day via Webstar.

IMPORTANT

Never share your password with anyone. You are personally responsible for any actions that are taken with your accounts.

Problem Issues With Passwords

If a user has set up a password and used it successfully signing in, but then encounters an error message, the user should first contact their agency Security Administrator or the Security Administrator Assistant to reset the password. If this situation cannot be remedied by the agency Security Administrator or Assistant, then the user can contact the NYS OFT Customer Care Help Desk (1-800-697-1323).

Security Information Access

Public Folders

The Public Folders contain information related to Key Users, LAN Administrators and Security Administrators such as who the LAN Administrator or Security Administrator is for agencies, as well as other information related to security. The path in the Public Folders is: Public Folders>All Public Folders>dfa.state.ny.us>User Account Services>OFTSEC>Forms>Weekly Reports. If the public folder does not appear at the bottom of the list of folders in Outlook, go to the bottom of the page and click on the icon that looks like a folder lying on its site.

OCFS Intranet

The OCFS intranet includes a page on Security information, which includes access to the Security Step by Step Guide, as well as other pertinent information related to OCFS security. It can be accessed by going to: http://ocfs.state.nyenet/it/security.