COM PASSWORD STANDARDS

With the implementation of a new COM Portal in January 2016, the IT department updated its password standards. The new password complexity requirement is necessary to ensure compliance with existing laws and regulations regarding data security and protecting the privacy of personal information.

Password Must:

1. 12 characters or more in length
2. No personal names
3. No common names or dictionary words
4. No sequences of more than 3 digits in a row
5. Must contain at least one character from the following four categories:

    - Uppercase alphabet characters (A–Z)
    - Lowercase alphabet characters (a–z)
    - Base 10 digits (0–9)
    - Non-alphanumeric characters (for example, ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Password Reset:

Use the following link from the MyCOM portal to reset your password

https://mycom.marin.edu/web/first-time-users/reset-password (https://mycom.marin.edu/web/first-time-users/reset-password)

Please do not attempt a password reset at any other website than at the MyCOM portal.

STAFF Only: Please keep in mind that changing your MyCOM password is effectively changing your network password. Your MyCOM and network username and password are the same. If you are logged onto a district PC with your network account, follow the steps below from the district PC. Do not use the MyCOM portal to change your password.

- Press Ctrl+Alt+Delete, and then click Change a password.
- Enter your current (i.e. old) password and a new password matching the conventions noted in Change Password below.
- Enter the new password a second time to confirm your first entry.
- Press the Next arrow.

Account Unlock:

If you attempt login too many time with a wrong password, your account will be automatically locked. This feature helps to prevent attackers from guessing users' passwords, and decrease the likelihood of successful attacks on your network.

- Account lockout threshold: after 10 failed logon attempts, your account will be locked for 15 minutes. You may reset your password after that wait period.
- Account lockout duration: your account will stay locked out for 15 minutes. Please wait for that duration before attempting the next login.

Password Best Practices

- Always use strong passwords.
- If passwords must be written down on a piece of paper, store the paper in a secure place and destroy it when it is no longer needed.
- Never share passwords with anyone.
- Use different passwords for all user accounts.
- Change passwords immediately if they may have been compromised.
- Be careful about where passwords are saved on computers. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember a password. Selecting this option poses a potential security threat.