Guidelines for Creating and Use of Computer Network Passwords

The following are general guidelines for recommendations for creating and using a Strong Password.

A Strong Password **should:**

- ✓ **Be a least 8 characters in length**
- ✓ **Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)**
- ✓ **Have a least 1 numerical character (e.g. 0-9)**
- ✓ **Have at least one special character (e.g. ~!@#$%^&*()**

A Strong Password **should not:**

- ✓ **Spell a word or series of words that can be found in a standard dictionary**
- ✓ **Spell a word with a number added to the beginning and the end**
- ✓ **Be based on any personal information such as family name, pet's name, birthday, etc.**

The following are recommendations for maintaining security of your Password:

- ✓ **Do not share your password with anyone for ANY reason**
    - Passwords should not be shared with anyone, including any students, faculty or staff, administration, or temporary/substitute personnel. Sharing a password for any reason may allow that permitted individual to unsafely discard of your network logon information. In situations where someone requires access another individual's protected resources, permission should be requested from district administration or NERIC staff.
- ✓ **Change your password periodically**
    - A strong policy to follow is change your password every 90 days. This will prevent someone, who has obtained your password through any means, from having continued access to your account. If you suspect someone has compromised your account, change your password IMMEDIATELY!
- ✓ **Consider using a passphrase instead of a password**
    - A passphrase is a password made-up of a sequence of words with numeric and/or symbols inserted throughout your password. A passphrase could be a lyric from a song or a famous quote. Passphrases usually exceed a safe password's length of 8 characters and most importantly, much easier to remember. An example may be "**L00k I can f$y!**" Notice the placement of the numbers, special symbols, and blank spaces prevent the multiple words being found in a standard dictionary and very difficult to guess.

- ✓ **Do NOT write your password down or store it in an insecure or obvious location.**
    - You should avoid writing down your password, but, if you must, all passwords should be recorded and stored in a secure location and shredded when no longer needed.
    - A password manager is strongly discouraged unless the manager uses strong encryption and requires two-step authentication.

- ✓ **Avoid reusing a password**
    - When changing your password every 90 days or when you suspect your account has been compromised, avoid using previous utilized passwords. Reused passwords could lead to continual access to your account due to the uncertainty of when your account was initially compromised.

- ✓ **Avoid using the same password for multiple accounts**
    - Passwords used on multiple accounts may seem convenient, but, not access to multiple accounts may be compromised as a result of one account's unauthorized access. Please do not use the same passwords that are used to access your personal accounts (e.g. bank accounts and investments). If fact, you should have different passwords for social media (Facebook & Instagram), professional accounts (LinkedIn), personal accounts, or other web-based accounts

- ✓ **Do NOT use automatic logon functionality**
    - When you create an account and then chose to have your password remembered, you are negating the primary value of using a password. If an unauthorized user gains access to your computer system where you have utilized automatic login, you could compromise personal and network information that is confidential resulting in information integrity and availability.

- ✓ **If you suspect your account(s) have been compromised, please contact a building administrator and District NERIC staff immediately!**