cornerstone

CORNERSTONE GUIDELINES FOR PASSWORDS

Network passwords are a critical element of your overall network security. They help protect your accounts and data, and strong passwords are necessary. Weak passwords, or no passwords, are a risk to your entire network. Cornerstone clients are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. If you need help or guidance in implementing a strong password policy, our team is able and eager to assist.

Three important factors this document covers are strong passwords, protecting those passwords, and changing those passwords periodically.

Strong Passwords

- Users must have a unique password from all other accounts held by that user, as well as a unique password from all other users on the network.
- Passwords should not be the same as the user ID.
- Passwords should have at least 8 characters.
- Passwords should have a mixture of both uppercase and lowercase letters.
- Passwords should have a mixture of both letters and numbers
- Passwords should include at least one special character (! $ # ? *).
- Do not have your web browser remember your passwords. Enter them each time.

Password Protection

- Passwords should not be transmitted via email messages or other forms of electronic communication.
- Any passwords that are no longer needed should be deleted. This applies when a user retires, quits, is dismissed, etc. This also applies to contractor accounts when that contractor is no longer needed to perform their duties.
- Passwords should not be displayed when entered.
- Do not share passwords with anyone, including administrative assistants. All passwords should be treated as sensitive, confidential information.
- Don't write passwords down and store them in your office.
- Don't store passwords on an unencrypted file on your computer.

Password Changes

- Passwords should be changed at least every 90 days, and you should not re-use old passwords.