1. **Use Complex Passwords:** This may seem basic. But simple passwords are easily compromised. Enforcing complexity requirements is a good first step in stopping brute force hacking attempts. You can require that all users create passwords that do not reference the user’s legal name or username. Robust passwords also utilize combinations of characters, numbers, as well as upper- and lower-case letters.
2. **Set Minimum Password Length:** You can boost the robustness of passwords within your organization, by setting a minimum character length. A common practice is a minimum of eight characters. A minimum character length of 14 characters is become a better standard.
3. **Utilize Passphrases:** Domain administrators’ accounts require greater protection. In such cases, passphrases (with a 15-character minimum length) are easier to remember and type, but harder to gain access to.
4. **Mandatory Password Resets:** For greater protection, it is common to have minimum reset periods.  This can also be varied for more critical functions within the organization.
5. **Restrict Password Reuse:**Recycling is good for the environment, but not for your company’s password management! Choosing to enforce the password history requirement will limit how often an old password can be used. Setting minimums, such as the previous 5 passwords not being allowed can help avoid the overuse of “favorite” ones.
6. **Set Minimum and Maximum Password Age Limits:** Sometimes employees will temporarily change a password and then switch back to a familiar one.  Requiring each password to be held for three to seven days eliminates this issue. However, your IT support should be available to change compromised passwords when the minimum age limit isn’t met. Setting a maximum password age limit also helps with network security. Usually, this is set anywhere from 90 days for passwords to 180 days for passphrases.
7. **Establish Password Audits:** You will need to track your team’s compliance with the password security policy. An audit will monitor password modifications to ensure compliance and to highlight and correct weak access points.
8. **Send Reminders:** Your team is likely to forget to comply with the company’s password policy on their own. Send email notifications to remind them to change their passwords before they expire.