611 Brookside Road
Suite 206
Victoria, B.C. V9C O3C

# Daxtech Default Network Security Setup

- **Why we do it the way we do**
  - Here is a list of configurations that we setup by default and an explanation as to why we do things the way we do.

    - No local admin rights
      - Having local admin rights on your computer, (although very convenient to install software and updates) creates a high security risk for your computer and the entire network. When a virus or malicious software is installed a computer, it takes on the access privileges of the currently logged in user. If that user account is an administrator, the virus has free range cause unlimited damage to the system. In addition, it can spread more easily throughout your entire network.

    - No admin rights for 3rd parties
      - Same as above we also be default to not allow admin access to your network for any third party companies such as your line of business software vendor (ie Sage, ESILAW etc) as this leaving another door open to potential risks of the account being used maliciously.

    - No admin passwords for clients without signed waiver of liability
      - Yes we are very security conscious but we realize your data is your data and your technology is yours to do whatever you wish. We will always give our best practice recommendations but if you wish to have full admin access to your network we will set this up without issue. We do however require a signed document waiving Daxtech of any responsibilities due to access no longer being solely in our control.

    - Web and content filtering where possible
      - In addition to protecting access to the local computers and network, we also by default setup website content filtering should you purchase one of our recommended firewall products. The cyber threats that exist online nowadays are becoming more and more sophisticated and malicious. Even websites that appear harmless can have code running in the background to infect computers that view them, without any intervention from the end user. It is for this reason that we enable filtering whereby site categories that are not necessary for your day to day business are blocked.

    - Strong 16 character passwords
      - Long complex passwords are now highly recommended. By default we will setup your network with this requirement to protect against brute force (automated password guessing) software. This is a very common method of attack and very successful on systems with weak passwords.

- We do not track user passwords
  - For your security and ours, we do not store staff user account passwords in our network documentation. Even IT service providers like us are vulnerable to cyber threats so we have made this important business decision in order to further protect our clients networks.

- Always use approach of granting access to only what is needed for user to do their job
  - Using a least privilege approach helps ensure that no doors are left open to your network unnecessarily. We will by default setup permissions for staff and authorized 3rd parties in such a way that access is only granted to what is necessary in order to do a job or task.

- **How this is beneficial to protect client networks**
  - The security of your network is our top priority and our methods are designed in such a way to minimize the attack points on your network and also to reduce the destructive capabilities of a malicious attack should one get through.

- **What if client wants administrative access to their network?**
  - We understand your network is your network and we don't want to restrict your access to your investment however being we work with business technology every day and see the damage todays cyber threats can cause, we feel we would be doing a disservice if we did not advise you of the potential risks. We have a form for you to sign which explains many of these risks in detail and also absolves Daxtech of any liabilities due to the existence of a secondary administrator account.