

General Security Guidelines

1. Don't save passwords locally.
 1. If your browser supplies your ID and password for you, anyone can use it.
 2. If your VPN product doesn't prompt for your password, anyone can use it.
2. Never "auto-login" your Desktop.
 1. Your Computer should ALWAYS prompt you for your user ID and password.
 2. The previous login should NOT be displayed.
3. Passwords should be hard.
 1. Passwords should be a minimum of 8 characters long, using a mixture of upper and lower case letters, numbers and special characters.
 2. Something more like a "passphrase" should be used. My Dog is Red = MyD0gizR3d!
4. Laptops can be lost or stolen. Encrypt your data using either the OS's built-in ability, or Third Party tools. Windows (EFS, BitLocker), Mac (FileVault), Third Party (TrueCrypt).
5. USB devices are easily lost. The devices need to offer encryption and password protection.
 1. Data should be encrypted using AES algorithms (TrueCrypt).
 2. Access should require a password.
6. Employ Screen savers.
 1. Screen saver should require a password to unlock.
 2. Set to invoke at 10 minutes.
7. For Windows, Ctrl-Alt-Delete must be required for Login.
8. Don't allow Print/peer to peer file sharing.
9. Use Anti-Virus and Anti-Spyware software.