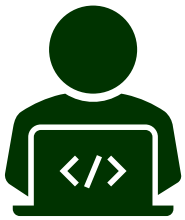
Page Wolfberg & Wirth
The National EMS Industry Law Firm

Secure Remote Working SAMPLE Policy

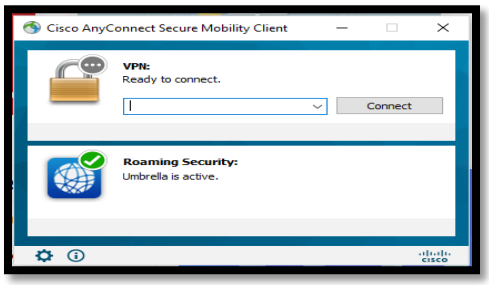
Device Security



- **Encryption**. All devices (laptops, PCs, etc.) used to access, receive, transmit or maintain company information must be encrypted. Talk to the IT department to ensure your remote devices are encrypted.

- **Company Approved**. You may only use company-approved devices to work remotely. Personal laptops, tablets, and other devices must be approved for remote use.

Secure Access

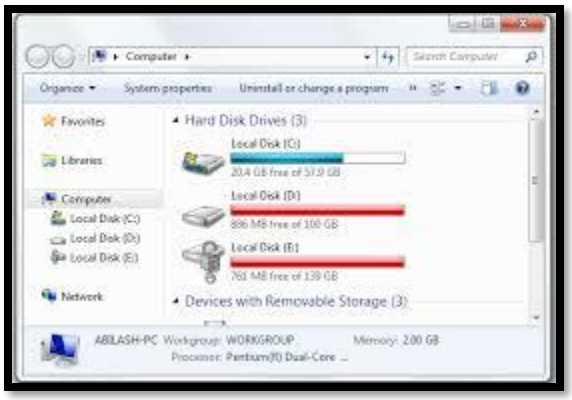


- **Username and Password.** You must have a unique username and password to log into company systems or applications and access company information.

- **Over the Internet.** You should always be connecting over Hypertext Transfer Protocol Secure (https) when accessing company information over the internet. Talk to management if you have questions about what websites you may access.

- **Our Servers**. You must connect through a Virtual Private Network (VPN) access to company servers and information systems.

No Local Downloading or Storage of Company Information



- **No Local Storage**. No company information should ever be downloaded, stored, saved or otherwise maintained locally, even for a brief second. This means no company information should be saved to any desktops, local drives, hard drives or local storage media (USB drives, external hard drives, etc.).

- **No Physical Copies.** No company information should be printed or otherwise maintained physically at a remote location without the express consent of management.