TELECOMMUTING SECURITY AND YOUR BUSINESS

A recent technology survey from the National Small Business Association reports that 44 percent of small businesses allow their employees to work remotely. While offering potential benefits, telecommuting also introduces new risks:

- Accessing unsecured public Wi-Fi networks
- Letting family and friends use work issued devices
- Altering security settings to view blocked sites
- Leaving work issued devices in an insecure location
- Backing up company data to a home computer
- Emailing company data to a personal email account

Securing devices

- Protected information must be transported in a secure manner.
- When transporting laptops, hard drives and other devices by car, be sure to lock the vehicle during any stops along the way. Electronic devices should not be left visible in the car.
- Protected information must be stored in a secure place away from public or family exposure/access.

Securing data

- Do not store data on non-company-owned computers.
- Dispose of any company documents according to company policy.
- Use network access control (NAC) systems to check clients and laptops to make sure they are hardened, secure and comply with your information security policies.
- Make sure all devices are patched, up-to-date and have protection like antivirus and antispyware software installed.

Wi-Fi security

- If you have a choice, select wireless networks that use some form of encryption. In order of preference, choose networks secured with WPA2 encryption, then WPA. Use WEP only as a last resort.
- After joining, set network location to “Public” (in Windows 7) to block file and printer sharing—common routes for hackers.
- Use a VPN (virtual private network) to access company servers. VPNs encrypt any traffic from the remote client to the corporate network, creating secure tunnels that prevent snoopers from intercepting data from your web sessions.
- Never opt to have your browser or a particular website ‘remember’ or ‘save’ your password.
- Use HTTPS and SSL connections whenever possible. Many websites use HTTPS and SSL to make your connection more secure—both protocols provide encryption. For example, *https://www.gmail.com* is more secure than *http://www.gmail.com*, which is unencrypted.

Before travelling

- Run a data scan to identify the nature and location of potentially confidential information such as Social Security or credit card numbers.
- Ensure your operating system is fully patched.
- Verify that your antivirus software has the latest virus definition updates.
- Update third-party software (e.g. Adobe).