Your Business IT Systems Manager
Managed BITS

# Managed BITS Network Security Check List

*How secure is your business IT network? Take a look through the below security categories and ensure your network is protected.*

- Anti-virus software: All notebooks, desktops and servers need Anti-virus software with current subscriptions and up-to-date security definitions. The threat of a virus infection could cause significant down-time, data loss and even data theft.

- Updates: Ensure your computers and servers have the latest operating system updates. These updates help prevent security exploits and can also provide additional features to your systems. Are you still using Windows 98 or 2000. These operating systems are no longer supported and do not receive any updates.

- Firewalls: Firewalls help to prevent unauthorised intruders gaining access to your network. Combinations of software and hardware firewalls are recommended for the greatest protection. It may be as easy as ensuring your Windows firewall is turned on and your router has firewall protection built in.

- Passwords: Is your password ‘password’? Or ‘123456’? Often overlooked passwords are very important to help protect your network. For the best results a password should be changed regularly, be over 8 characters and comprise of numerical and uppercase letters at a minimum.

- Spam: Do you receive a large amount of spam emails? Does your network have appropriate spam filters in place? Spam emails are one of the greatest threats to your network and spammers are consistently trying new ways of getting into your inbox. Ensure your network has appropriate spam detection software or emails are being filtered using online services.

- Folder and file restrictions: Do all staff have access to all folders and files in the network? Can they access HR or financial information? It’s important access levels are associated with various staff members. This could help prevent a disgruntled employee deleting or stealing unprotected company information.

- Education: Do all users know how to keep their information secure? Browse the internet safely and understand what they can and cannot do on business computers? The biggest threat to a business network is the users themselves. Users need to be correctly educated and aware of company IT processes and procedures.

- Software:  Out-dated software can provide easy access for intruders. Network preventative maintenance should often be carried out. This will ensure old software especially remote access programs are removed or updated to their latest version.