

# Computer Security Checklist

By Alex Strickland

- Data Backup
  - Perform regular backups of all data files.
  - Test restoration of client data files to ensure the backup files work.
  - Make sure at least one copy of the data is stored in a secure, off-site location.
  - Review your backup requirements periodically.
- Physical Security
  - Make sure your computers are located in areas that are not easily accessible to outsiders.
  - Make sure you and your staff take responsibility for locking doors and windows.
  - Check if your desktop and laptop computers are equipped with anti-theft devices.
  - Check if your network servers are physically secure in a separate area.
  - Make sure you have an accurate inventory of all computing equipment and software that is stored off-site.
  - Implement a "clear desk" policy to ensure your staff secures sensitive and confidential files when they're not working on them.
- Virus Protection
  - Check if anti-virus software is installed on all your computers.
  - Check if anti-virus software been configured to check all mediums (email, web sites, downloaded files) for viruses.
  - Check if a procedure for automatically updating the anti-virus software is in place.
  - Check if users know what to do when infected with a computer virus.
  - Make sure you and your staff open only attachments they expect.
- Disaster Recovery
  - Have written continuity plan in place in the case of a major disaster (like fire).
  - Check how long your practice could function without computers, servers, or network access.
  - Check if your head office provide any disaster recovery assistance.

- Make sure you have at least one copy of client data and application software stored in a secure, off-site location.
- Make sure you have a current inventory of your computer equipment, software, and critical client files.
- Firewall
  - Check if all of your computers have firewall software installed.
  - Make sure the firewall software been configured to protect the required information on your computers.
  - Check if your network have a hardware firewall installed.
  - Check if you have firewalls installed at every point where your computer systems is connected to other networks.
- Password Management
  - Require passwords for access to all computers.
  - Choose "strong" passwords.
  - Change passwords regularly.
  - Make sure that passwords are not written down or shared.
  - Prevent users from choosing passwords that have been used only a short while ago.
  - Deactivate accounts for terminated employees in a timely manner.
- Miscellaneous
  - Don't store sensitive information on USB drives
  - Frequently clear private data from Web browsers.
  - Make sure your operating system is updated.
  - Use a password-protected screen saver or 'lock' the screen.