CYBERSECURITY CHECKLIST

- [ ] Does a director or equivalent have responsibility for Data Protection?
- [ ] Has the company assigned the responsibility of Data Protection Officer to an individual?
- [ ] Have all the staff given written acknowledgment that they have read, understood and accepted your data protection and security policy?
- [ ] Do all computer users in the company receive regular training in their security responsibilities and what to do if they identify security threat?
- [ ] Are firewalls and routers regularly tested for vulnerabilities?
- [ ] Has a crisis plan been put in place to ensure the company acts appropriately to any security breaches?
- [ ] Are users forced to change passwords on a monthly basis and also forced to use complex passwords?
- [ ] Are systems and databases that store personal data secured properly to ensure compliance with regulatory and legal requirements such as the Data Protection Act?
- [ ] Are all systems protected with the most up to date anti-virus software?
- [ ] Are both emails and internet browsing activity monitored to protect the Company from computer viruses?
- [ ] Are the log files of security devices actively monitored to detect potential Security breaches?
- [ ] Are IT resources such as servers located in a secured area to avoid unauthorised access?