

# CYBER SECURITY KEY CONSIDERATIONS

01		When did you last review your cyber security policy?	<input type="checkbox"/>
02	****	Is your password setting protocol complex enough, and enforced throughout your company?	<input type="checkbox"/>
03		Do you backup your data frequently and in different locations both online and offline?	<input type="checkbox"/>
04		Are you and your staff trained on phishing scams by emails, phone calls and texts?	<input type="checkbox"/>
05		Do you have a mobile working policy in place?	<input type="checkbox"/>
06		Do you ensure your remote connections are secure?	<input type="checkbox"/>
07		How do you ensure the personal information of staff and customers is protected (name, address, D.O.B and any identity numbers)?	<input type="checkbox"/>
08		How do you manage folder permissions? Can staff only access what they need?	<input type="checkbox"/>
09		How often do you run staff training for cyber security?	<input type="checkbox"/>
10		Do you update your digital products to keep your secure from the newest forms of attacks?	<input type="checkbox"/>
11	✓✓✓	Do you use multi-factor authentication as an additional layer of protection?	<input type="checkbox"/>
12		Who takes care of your cyber security? Do they expert qualifications and experience?	<input type="checkbox"/>
13		Do you have a robust disaster recovery plan place?	<input type="checkbox"/>