|  |
| --- |
| **CYBER LIABILITY ENQUIRY FORM** |
| Name of Insured (including all trading names): |  |
| **Cyber Liability** limit of indemnity required (please advise if higher limits are required): £100,000 [ ]  £250,000 [ ]  £500,000 [ ]  £1,000,000 [ ]  |
| **Optional Extensions** |
| **Cyber Business Interruption** limit of indemnity required (inner limit being part of and not in addition to the total limit of liability):£100,000 [ ]  £250,000 [ ]  £500,000 [ ]  £1,000,000 [ ]  Not required [ ]  |
| **Social Engineering Fraud** limit of indemnity required (maximum 10% of the total Cyber Liability limit capped at £50,000):£10,000 [ ]  £25,000 [ ]  £50,000 [ ]  Not required [ ]  |
| **Risk Questions** | **YES** | **NO** |
| Does the company have a website | [ ]  | [ ]  |
| Website address: |  |
| Percentage of turnover generated online |  |
| Have you had any cyber or data breach incidents or other incidents that would otherwise have been covered under this policy had it been in force at the time  | [ ]  | [ ]  |
| Have you previously sustained any unscheduled or unintentional network outage  | [ ]  | [ ]  |
| Are you compliant with the Payment Card Industry Data Security Standards  | [ ]  | [ ]  |
| Do you have Anti-Virus software and Anti Spyware installed and updated in accordance with suppliers recommendations  | [ ]  | [ ]  |
| Do you have a firewall in place for all external gateways and updated in accordance with suppliers recommendations  | [ ]  | [ ]  |
| Do you use multi-factor authentication (MFA) for the following; |
| Cloud based services (such as cloud-based email account access)  | [ ]  | [ ]  |
| All remote access to your network  | [ ]  | [ ]  |
| Internal administrative access to directory services, backups, infrastructure and endpoints  | [ ]  | [ ]  |
| None of the above  | [ ]  | [ ]  |
| Do you allow remote access into your environment without a virtual private network (VPN)  | [ ]  | [ ]  |
| Do you regularly (at least annually) provide cyber security awareness training, including anti-phishing, to all individuals who have access to your organisation's network or confidential/personal data  | [ ]  | [ ]  |
| Do you back-up critical data to a "cold" or "offline" location that would be unaffected by an issue with your live environment  | [ ]  | [ ]  |
| Do you test to ensure those backups are recoverable  | [ ]  | [ ]  |
| Estimated total number of individuals (including prospective, current and former customers and employees) where records are stored and/or transacted containing any individual personal, financial or sensitive information |  |
| **Details of disclosures above (including claims and incidents)** |
|  |