Cyber Insurance – Statement of Facts

Applicant Name:			
Applicant Address:			
Country of Domicile:	USA	**Website Address:**	
Nature of Business:			

Financial Information	**Last Complete Financial Year**	**Current Year (Estimate)**	**Next Year (Estimate)**
Gross Annual Revenue		**$**	**$**

Declarations – ***Sign & date below to acknowledge agreement with the following statements:***		
1	Access to all servers, firewalls, and IT infrastructure components has been restricted to appropriate personnel only.	
2	You take backups at least weekly which are stored separate from your network, e.g. off-line or with a specialist cloud hosting service.	
3	Within the last year you have successfully restored data from your backups.	
4	You have one or more firewalls protecting external access to your systems.	
5	All system users have individual, mandatory and non-trivial user IDs and passwords.	
6	All employees receive awareness training or educational information relating to phishing and other types of attacks.	
7	You protect all PCs and servers with anti-virus that you update regularly.	
8	You protect all remote access, including access to cloud environments and MS Office 365 if used, with encrypted connections such as a VPN.	
9	You have deployed MFA for all remote access, including access to cloud environments and MS Office 365 if used.	
10	You store less than 250,000 Personal Identifiable Information records (one record equals one person).	
11	Payment card data never passes through and is never stored within your networks or systems.	
12	You have a disaster recovery plan that you test at least annually.	
13	You have a process to review all content prior to posting on your Intranet Sites, Internet Sites or on social media that includes checks for disparagement, copyright infringement and trade mark/trade name infringement.	
14	You are not aware of any cyber incidents, personal information compromises, privacy violations, unscheduled network outages, copyright issues or other incidents or events that could give rise to a claim under a cyber policy.	
15	Do you store or process payment card data? (If yes, please answer the Payment Card questions)	☐ **Yes** ☐ **No**
16	Do you store or process healthcare data? (If yes, please answer the Healthcare questions)	☐ **Yes** ☐ **No**

By signing this form, you agree with all statements 1 through 16 above and the Payment Card or Healthcare questions below, where necessary.

Name	**Signature**	**Position**	**Date**

Payment Card Questions - ☐ **N/A**		
1.	You outsource payment card processing to a specialist payment card processor.	☐ **Yes** ☐ **No**
2.	You are Payment Card Industry Data Security Standards compliant against PCI Version 3x standard.	☐ **Yes** ☐ **No**
3.	Payment card data is stored within your systems or networks.	☐ **Yes** ☐ **No**
4.	Payment card transactions are encrypted from point-of-sale and through the whole payment process.	☐ **Yes** ☐ **No**

Healthcare Questions - ☐ **N/A**		
1.	You are HIPAA compliant.	☐ **Yes** ☐ **No**
2.	You encrypt all Personal Health Information stored on portable media and devices.	☐ **Yes** ☐ **No**
3.	All employees with access to healthcare information receive HIPAA awareness training at least annually	☐ **Yes** ☐ **No**