Allied Health

Cyber Insurance Proposal Form

1. Business Entity Name:
2. ABN:
3. Occupation/Business Description:
4. Business Address:
5. Association (if applicable):
6. Annual Turnover:
7. Turnover split by state / territory (%):

NSW:		**VIC:**		**QLD:**	
WA:		**SA:**		**ACT:**	
TAS:		**NT:**		**Overseas:**	

8. Cyber Liability Aggregate Policy Limit Required: ☐ **$250K** ☐ **$500K**
9. Business Website Domain:
10. Email Address:
11. Number of Employees:
12. Do you implement encryption on laptop computers, desktop computers, and other portable media devices? ☐ **Yes** ☐ **No**
13. Do you collect, process, store, transmit, or have access to any Payment Card Information (PCI), Personally Identifiable Information (PII) other than your employees? ☐ **Yes** ☐ **No**

If Yes,

a) How many PII records does your business collect, process, store, transmit, or have access to? ☐ **None** ☐ **<100K** ☐ **100K to 500K**

b) What is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)? ☐ **None** ☐ **<100K** ☐ **100K to 500K**

Allied Health

Cyber Insurance Proposal Form

14. Do you have a security tool protecting computers and handheld devices (Anti-Virus Software, Anti-malware, Endpoint Detection and Response)? ☐ Yes ☐ No

15. For which of the following services do you enforce Multi-Factor Authentication (MFA)?

    a) Email ☐ Yes ☐ No

    b) Virtual Private Network (VPN), Remote Desktop Protocol (RDP), RDWeb, RD Gateway, or other remote access ☐ Yes ☐ No

    c) Network / cloud administration or other privileged user accounts ☐ Yes ☐ No

16. Does your business require a secondary means of communication to validate the authenticity of:

    a) Funds transfer requests (ACH, wire, etc.) before processing a request in excess of $2,000 ☐ Yes ☐ No

    b) Any request to change banking details (ACH, wire, payroll distribution, etc.)? ☐ Yes ☐ No

17. Do you maintain weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a seperate network? ☐ Yes ☐ No

18. During the past three years, did your business experience a cyber incident, claim or loss, whether insured or not, which could have been covered under a policy similar to the proposed insurance, this includes but is not limited to any:

    a) Actual or reasonably suspected data breach or security failure, including notifying consumers or third parties of a data breach or security failure ☐ Yes ☐ No

    b) Claims or complaints with respect to privacy injury, breach of information or network security, unauthorised disclosure of information, defamation, or content infringement ☐ Yes ☐ No

    c) Government action, investigation, or subpoena regarding any alleged violation of a privacy law or regulation; or ☐ Yes ☐ No

    d) Actual or attempted extortion demand with respect to its data or computer systems ☐ Yes ☐ No

Allied Health

Cyber Insurance Proposal Form

19. Are you aware of any circumstance that could give rise to a claim under this insurance policy? ☐ Yes ☐ No

20. Do you have knowledge or information regarding any fact, circumstance, situation, or event that could reasonably give rise to a claim or loss under the proposed insurance? ☐ Yes ☐ No

If yes, please explain the incidents / or claims.
Where possible details should include the date of the event, date of notice to your insurer, name of insurer, if you involved law enforcement, description of the circumstances or potential claim and current status.

21. What date would you like the policy to start from?

Once completed, please send this form to: **newenquiries@insurance.com.au**