360 Cyber

Mid-Market Cyber Insurance Proposal Form

360 Financial Lines Pty Ltd **ABN** 72 629 145 357 is an Authorised Representative (**AR** 1268172)
of 360 Underwriting Solutions Pty Ltd **ABN** 18 120 261 270 **AFSL** 319181
Suite 1, Level 18, 201 Kent Street, Sydney, NSW 2000

Important Information

The information you provide in this document and through any other documentation, either directly or through your insurance broker, will be relied upon by us and the Insurers to decide whether or not to accept your insurance as proposed and if so, on what terms.

Every question must be answered fully, truthfully and accurately. If space is insufficient for your answer, please use additional sheets, sign and date each one and attach them to this document.

If you do not understand or if you have any questions regarding any matter in this document please contact us or your insurance Broker before signing the Declaration at the end of this document.

Unless we have confirmed in writing that temporary cover has been arranged, no insurance is in force until the risk proposed has been accepted in writing by us and you have paid or agreed to pay the premium.

Agent of Insurers

360 Financial Lines Pty Ltd (360 Financial Lines) is an authorised representative (**AR** 1268172) of 360 Underwriting Solutions Pty Ltd (360 Underwriting Solutions) and has developed this Cyber Insurance Policy which is underwritten by certain Underwriters at Lloyd's. 360 Financial Lines acts as an agent for certain Underwriters at Lloyd's and is authorised to arrange, enter into/bind and administer this insurance for them and not as your agent when issuing insurance policies, dealing with or settling any claims.

Claims Made and Notified Policy Cover

The proposed insurance is issued on a 'claims made and notified' basis. This means the policy responds to:

+ claims first made against you during the policy period and notified to us during that policy period, providing that you were not aware, at any time prior to the policy inception, of circumstances which would have alerted a reasonable person in your position that a claim may be made against you; and
+ 'facts that might give rise to a claim against you' notified to us pursuant to Section 40 (3) of the *Insurance Contracts Act 1984 (Cth)*. This Section states, 'where the insured gave notice in writing to the insurer of facts that might give rise to a claim against the insured as soon as was reasonably practicable after the insured became aware of those facts but before the insurance cover provided by the contract expired, the insurer is not relieved of liability under the contract in respect of the claim, when made, by reason only that it was made after the expiration of the period of the insurance cover provided by the contract'.

After expiry of the policy, no new claims can be made on the expired policy even though the act / error / omission giving rise to the claims may have occurred during the policy period.

If during the policy period you become aware of facts or circumstances which a reasonable person in your position would consider may give rise to a claim against you, and you fail to notify to us during the policy period, we may not cover you under a subsequent policy for any claim which arises from these facts or circumstances.

When completing this Proposal Form you are obliged to provide full details of all facts or circumstances of which you are aware and which a reasonable person in your position would consider may give rise to a claim.

It is important that you make proper disclosure (see Duty of Disclosure) so that your cover under any policy issued by us is not compromised.

Duty of Disclosure

Before you enter into this insurance with us, you have a duty of disclosure under the *Insurance Contracts Act 1984 (Cth)*.

This means you have a duty to tell us every matter you know or could reasonably be expected to know that may affect our decision to offer you insurance and on what terms. If you are not sure whether something is relevant, you should inform us anyway.

You have a different duty the first time you enter into a contract of insurance with us to that which applies when you vary, renew, extend or reinstate the contract. This duty of disclosure applies until the contract is entered into (or renewed, varied, extended or reinstated as applicable).

Your Duty of Disclosure when you enter into the contract with us for the first time

If we ask you questions that are relevant to our decision to insure you and on what terms, you must be honest and tell us anything that you know and that a reasonable person in the circumstances would include in answer to the questions. It is important that you understand you are answering our questions in this way for yourself and anyone else that you want to be covered by the contract.

Your Duty of Disclosure when you renew the contract

Where applicable, we will tell you what your renewal duty of disclosure is prior to each renewal.

Your Duty of Disclosure when you vary, extend or reinstate the contract

When you vary, extend or reinstate the contract with us, your duty is to tell us every matter that you know, or could reasonably be expected to know, is relevant to our decision whether to accept the risk of the insurance and, if so, on what terms.

What you do not need to tell us

You do not need to tell us anything that:

+ reduces the risk we insure you for; or
+ is common knowledge; or
+ we know or should know as an insurer; or
+ we have indicated we do not want to know.

If you do not tell us something

If you do not tell us anything you are required to tell us, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both. If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

Privacy

We are committed to protecting your privacy in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

The information provided in this document and any other documents provided to us will be dealt with in accordance with our Privacy Policy. By executing this document, you consent to the collection, use, storage and disclosure of your personal information in accordance with our Privacy Policy. If you do not provide the personal information requested or consent to its use and disclosure in accordance with our Privacy Policy, your application for insurance may not be accepted, we may not be able to administer our services/products, or you may be in breach of your duty of disclosure.

Our Privacy Policy explains how we collect, use, hold, disclose and handle your personal information including transfer overseas and provision to necessary third parties as well as your rights to access and correct your personal information and make a complaint for any breach of the APPs.

A copy of our Privacy Policy is located on our website at www.360uw.com.au.

Please access and read this policy. If you have any queries about how we handle your personal information or would prefer to have a copy of our Privacy Policy mailed to you, please ask us.

If you wish to access your file, please ask us.

360 Cyber

Section A. Company Information

Period of Insurance from / / to / /

Name

Address

Business description

Website(s) or domain(s)

Date established / /

ABN

Number of employees

Is the Company a subsidiary, franchisee or part of a larger group? Yes No

If yes, please provide details

Point of contact

Section B. Revenue

1. Please give the revenue generated from sales to the following:

Country	Revenue Generated
Australia	$
US	$
UK	$
EU	$
New Zealand	$
Rest of World	$

2. What percentage of your revenue is delivered from on-line sales?

3. Do you have any overseas subsidiaries? Yes No

If yes, please provide details

360 Cyber

Section C. Data Storage

1. Please provide the number of data records stored/processed by the Company or/and under Company custody:

Name	Number of Records	Information Stored	
Personal Data e.g. Name, Address, Email		Yes	No
Passport, Driving licence, Tax or Social Security numbers		Yes	No
Medical records, Healthcare Information		Yes	No
Biometric information, i.e. fingerprint, voiceprint		Yes	No
Financial (not credit or debit cards)		Yes	No
Payment Card Industry (credit and debit cards)		Yes	No

2. Do you encrypt all sensitive data held as defined above while:
   - – In transit? Yes No
   - – Stored on servers? Yes No
   - – Stored on portable media? Yes No
   - – Stored in backup? Yes No

Section D. Network Security

1. Who has overall responsibility for network security? Internal MSP
2. Do you have a documented baseline security framework across all operations, entities, subsidiaries, including international locations? Yes No
3. Do you undertake an internal or external security policy review or audit, at least annually? Yes No
4. Do you conduct vulnerability assessments or penetration testing? Yes No
5. Do you deploy the following applications/software across all endpoints and servers? Yes No
   - – Business Grade Anti-virus/Firewall Yes No
   - – Endpoint Detection and Response (EDR) Yes No
   - – Security Information and Event Management (SIEM) Yes No
   - – Security Operations Centre Monitoring (SOC) Yes No
   - – Web Application Firewall (WAF) for online applications Yes No
   - – Application Whitelisting Yes No
6. How often do you install critical patches?
   Automatically Daily Weekly Monthly Other
7. Do you run any software or hardware that is no longer supported by the manufacturer (End of Life)? Yes No
   If YES to the above, is it Segmented from the rest of the Network? Yes No
8. Do you segregate your network by geography, or business unit to isolate any potential malware infections? Yes No
9. Do you segregate your Operational Technology environment from your Information Technology network? Yes No

Section E. Access Controls

1. Is Multi-Factor Authentication (MFA) required for user access to:
   - – All remote access to your network, including via VPN and RDP ☐ Yes ☐ No
   - – Domain Admin and Privileged Access ☐ Yes ☐ No
   - – Backup and Cloud Environments ☐ Yes ☐ No
   - – All remote access to your Operational Technology Environment ☐ Yes ☐ No
2. Have you disabled Remote Desktop Protocol on all of your endpoints, and servers, unless protected by MFA? ☐ Yes ☐ No
3. Do you have a password policy requiring regular changes, password manager software or Single Sign On functionality for all users? ☐ Yes ☐ No
4. Is access to sensitive data restricted according to the employee's user requirements? ☐ Yes ☐ No
5. Do you automatically revoke all IT access for staff on leaving your employment? ☐ Yes ☐ No
6. Are Domain Admin and Privileged Access rights:
   - – Restricted to individual users based on requirements ☐ Yes ☐ No
   - – Protected with Privilege Management Access tools (PAM) ☐ Yes ☐ No

Section F. Business Continuity

1. Do you have a Business Continuity Plan (BCP) or Incident Response Plan (IRP) in place inclusive of cyber risk, which is tested at least annually? ☐ Yes ☐ No
2. Do you back up data necessary to run your business and test the backups at least annually? ☐ Yes ☐ No

   If YES, are your backups stored in an isolated environment, such as cloud or offline? ☐ Yes ☐ No
3. How often do you back up your data?

   ☐ Daily ☐ Weekly ☐ Monthly ☐ Other
4. After how long will your business be impacted by an interruption to, or total loss of, your network?

   ☐ >6hr ☐ 6–12hrs ☐ 12–24hrs ☐ >48hrs
5. How long will it take to fully restore your critical systems? (Recovery Time Objective)

   ☐ >6hr ☐ 6–12hrs ☐ 12–24hrs ☐ >48hrs

Section G. Email Security

1. Do you use any of the following to authenticate your email:
   - – SPF? ☐ Yes ☐ No
   - – DKIM? ☐ Yes ☐ No

   If so, do you also use DMARC? ☐ Yes ☐ No
2. Do you use Office 365? ☐ Yes ☐ No

   If "yes", do you use the O365 Advance Threat Protection add-on, or similar alternative product? ☐ Yes ☐ No
3. Do you scan incoming email for malicious attachments or links? ☐ Yes ☐ No
4. Do you provide training to assist employees in spotting phishing and other social engineering attacks, at least annually? ☐ Yes ☐ No

Section H. Payment Card Industry Compliance

(Note, even if you completely outsource your entire card data processing to a validated third party, you may still need to be compliant with PCI DSS rules and complete a Self-Assessment Questionnaire)

1. Are you in Compliance with the Payment Card Industry Data Security Standards? ☐ N/A ☐ Yes ☐ No
2. What level of merchant?
   ☐ 1 ☐ 2 ☐ 3 ☐ 4
3. Date of last audit
   / /

Section I. Russia, Ukraine, Belarus Exposure

1. Do you have any exposure in Russia, Ukraine, Belarus, i.e. subsidiaries, offices? ☐ Yes ☐ No

Section J. Claims

1. Have you suffered any unplanned outage, not caused by a power failure, of more than 4 hours in the last 24 months that may have resulted in a claim under a cyber policy if one was in force? ☐ Yes ☐ No

   If yes, please provide details

2. During the last 36 months has any sensitive or personal data for which you are legally liable been compromised or lost? ☐ Yes ☐ No

   If yes, please provide details

Section K. Stamp Duty

For the calculating of stamp duty payable on premium, please provide a geographical breakdown of income

NSW	VIC	QLD	SA	WA
%	%	%	%	%
TAS	**NT**	**ACT**	**O/S**	**Total**
%	%	%	%	%

Section L. Limit Required

Please select Limit of Liability required

☐ $1M ☐ $2M ☐ $3M ☐ $5M

Section M. Optional Extensions

Please indicate if you require cover under the following extensions of cover

Funds Transfer Fraud	☐	Combined Crime and Social Engineering Cover	☐	Crime Only Cover	☐	None			
Limit required	☐	25,000	☐	50,000	☐	100,000	☐	200,000	☐ 250,000
Telephone Hacking	☐	Yes	☐	No					
Limit required	☐	100,000	☐	200,000	☐	250,000			

If Funds Transfer Fraud Optional Cover is selected please complete the below questions:

1. Do you have a written procedure whereby, all new (including changes to existing) payment details or contact details are confirmed by an alternative method to the original method used, before any payment is made? ☐ Yes ☐ No
2. Do you maintain procedures, at least annually, for the provision of written training materials to all employees relating to the dangers of social engineering fraud, phishing and cyber fraud? ☐ Yes ☐ No

Declaration

I/we declare that to the best of my/our knowledge and belief the answers given on this Proposal whether by me/us or on my/our behalf are complete and true and that we have not withheld any material information.

I/we authorise 360 Financial Lines and the Insurer(s) it acts as agent for to give to or obtain from other insurers or insurance reference bureaus or credit reporting agencies, any information about this insurance or any other insurance of mine including this completed Proposal and my insurance claims history and my credit history.

Signature

Position

Print Name

Date

/ /

360CYMMPFV125

Suite 1, Level 18
201 Kent St
Sydney, NSW 2000