360 Cyber

Cyber Insurance Proposal Form

Date of preparation: 2 December 2024

Effective date: 1 January 2025

360CYPFV824

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.

Policy Details

Period of Insurance from / / to / /

Proposer

Address

Website URL (if not applicable, please write N/A)

Email Domain (if not applicable, please write N/A)

Business description

Are you a Franchisee or Franchisor? Yes No

ABN

Number of employees

Annual revenue for the last 3 years

This year	Last year	2 years ago
$	$	$

Is more than 25% of your revenue from the USA? Yes No

Do you have any financial nexus, financial agreements or contractual associations to countries other than Australia or New Zealand? Yes No

If yes, please list the countries you have any financial nexus, financial agreements or contractual associations with other than Australia or New Zealand.

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

NSW	VIC	QLD	SA	WA
%	%	%	%	%

TAS	NT	ACT	O/S	Total
%	%	%	%	%

All risks:

1. Do you deploy an active business grade firewall at all external gateways of your network and an active business grade antivirus application across your entire network, including servers or endpoints? Yes No
2. Do you (or your cloud service provider) backup your data to an isolated environment at least every 7 days and test it at least every 365 days.? Yes No
3. Do you secure all remote access to your network with a minimum of multifactor authentication? Yes No
4. Do you install critical patches within 30 days of release? Yes No

5. Have you suffered any loss or has any claim been made against you or are you aware of any matter that is reasonably likely to give rise to any loss or claim in the last 36 months where you would seek an indemnity from our cyber insurance policy? ☐ Yes ☐ No

If turnover is above $30M:

6. Is all personal data on individuals (PCI, PII, PFI and / or PHI) encrypted whilst on, and in transmission from your network? ☐ Yes ☐ No

7. Have you disabled Remote Desktop Protocol (RDP) on all your network's endpoints, including servers, unless protected by MFA? ☐ Yes ☐ No

Limit Required

Please select Limit of Liability required

☐ 100,000 ☐ 250,000 ☐ 500,000 ☐ 1,000,000 ☐ 2,000,000 ☐ 5,000,000

Would you like a Kynd Report run for this client? ☐ Yes ☐ No

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:

8. 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

9. 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

Additional Questions Dependent on Occupation

+ For Manufacturing see page 7
+ For Financial Institutions see page 7
+ For Renewable Energy, Power Generation and Utilities see page 7
+ For T.V., Broadcasting, Publishing, Music, Creative Arts and Advertising see page 7
+ For Education (including Childcare / Early Learning Centers) see page 8
+ For Heathcare and Professions (including Allied Health) see page 8
+ For Technology and Telecommunications see page 8
+ For Wholesaling, Online Retailing, Transport, Logistics, Warehousing see page 9
+ For Legal Professionals and Accountants see page 9

IF NONE APPLY, GO TO DECLARATION

Manufacturing

If annual revenue exceeds $30,000,000 please complete the below questions:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. Do you employ application white-listing? ☐ Yes ☐ No
4. Do you have any end of life hardware or software? ☐ Yes ☐ No
   a. And if so are they isolated from the network if airgapped/segregated from the rest of the network? ☐ Yes ☐ No
5. Is your operation technology environment segregated from your IT systems? ☐ Yes ☐ No

Financial Institutions

If annual revenue exceeds $30,000,000 please complete the below questions:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____
4. Do you have any end of life hardware or software? ☐ Yes ☐ No
   a. And if so are they isolated from the network if airgapped/segregated from the rest of the network? ☐ Yes ☐ No

Power Generation and Utilities

If annual revenue exceeds $30,000,000 please complete the below questions:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____
4. Do you employ application white-listing? ☐ Yes ☐ No
5. Do you have any end of life hardware or software? ☐ Yes ☐ No
   a. And if so are they isolated from the network if airgapped/segregated from the rest of the network? ☐ Yes ☐ No

T.V., Broadcasting, Publishing, Music, Creative Arts and Advertising

All risks:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____

Education

If annual revenue exceeds $10,000,000 please complete the below questions:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____
4. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ☐ Yes ☐ No
5. Do you have contractual (indemnity) arrangements with any Outsource or Cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ☐ Yes ☐ No
6. Is there a single policy governing all individual departments to control network and data security run by one department / provider? (Yes – i.e. School Head of IT or one MSP) ☐ Yes ☐ No
7. Have you disabled Remote Desktop Protocol (RDP) on all your network's endpoints, including servers, where RDP is not required? ☐ Yes ☐ No
   a. If not, is access restricted only through VPN, network level authentication and Multifactor authentication (MFA)? ☐ Yes ☐ No
8. Is all personal data encrypted whilst in transit, backed up and at rest on your network? ☐ Yes ☐ No

Healthcare and Professions

If annual revenue exceeds $30,000,000 please complete the below questions:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____
4. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ☐ Yes ☐ No

Technology and Telecommunications

All risks:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____
4. Do you conduct and processing or hosting activities? ☐ Yes ☐ No

Wholesaling, Online Retailing, Transport, Logistics, Warehousing

If annual revenue exceeds $30,000,000 please complete the below questions:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process? _____
4. What percentage of your revenue is delivered from online sales? _____ %

Legal Professionals

All risks:

1. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA? ☐ Yes ☐ No
2. Do you deploy either SPF, DKIM or DMARC? ☐ Yes ☐ No
3. How many records of personal data on individuals (PCI, PII, PFI and/or PHI) do you collect, store and process? _____
4. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ☐ Yes ☐ No
5. Do you have contractual (indemnity) arrangements with any Outsource or Cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ☐ Yes ☐ No
6. Is all personal data encrypted whilst in transit, backed up and at rest on your network? ☐ Yes ☐ No
7. Have you disabled Remote Desktop Protocol (RDP) on all your network's endpoints, including servers, where RDP is not required? ☐ Yes ☐ No
   a. If not, is access restricted only through VPN, network level authentication and Multifactor Authentication (MFA)? ☐ 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

/ /

360CYPFV824

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