



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 3, 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

Business Description

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

For the purposes 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 a business grade firewall at all external gateways of your network and a business grade anti-virus application across your entire network, including servers or endpoints? Yes No
2. You install critical patches within 30 days of release. Yes No
3. Data that is necessary to run the business is backed up by you (or your Cloud Service Provider) at least every 7 days. Yes No
4. This backed up data is stored in an environment which is completely separate to your network and its integrity is tested at least every 180 days. Yes No
5. Where applicable you are compliant with the Payment Card Industry (PCI) Data Security Standards? Yes No
6. Are you aware of any matter that is likely to give rise to any loss or claim, or have you suffered any loss, or has any claim been made against you in the last 24 months which you would seek an indemnity for under our cyber insurance policy? If yes, please provide details. Yes No

If annual revenue is above \$15,000,000 and under \$30,000,000 please complete the below question:

7. You secure remote access to your applications that are necessary to run your business with a minimum of 2 factor authentication. Yes No

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

8. You have disabled Remote Desktop Protocol on all your network endpoints, including servers, where RDP is not required. Yes No
9. All personal data is encrypted whilst on, and in transmission from, your network. Yes No
10. You secure remote access to your network and personal data with a minimum of 2 factor authentication. Yes No

Limit Required

Please select Limit of Liability required

- 100,000 250,000 500,000 1,000,000 2,000,000

Optional Extensions

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

- Funds Transfer Fraud Yes No
- 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 for validating all changes to vendor/client/customer contact details and/or bank account details in writing and then over the telephone with oral confirmation from the relevant employee/partner/director of the Insured or vendor/client/customer before the changes are actioned? Yes No
2. If yes, is that written procedure always followed? Yes No

Additional Questions Dependent on Occupation

- + For **Manufacturing** see page 7
- + For **Financial Institutions** see page 8
- + For **Power Generation and Utilities** see page 9
- + For **T.V., Broadcasting, Publishing, Music, Creative Arts and Advertising** see page 10
- + For **Education** see page 11
- + For **Healthcare Centres and Professions** see page 12
- + For **Technology and Telecommunications** see page 13
- + For **Wholesaling, Online Retailing, Transport, Logistics, Warehousing** see page 14
- + For **Legal Professionals** see page 15
- + If none apply, jump to declaration

GO TO DECLARATION

Manufacturing

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

1. Have you deployed the following security protocols
 - I. Sender Policy Framework (SPF) and or
 - II. Domain Keys Identified Mail (DKIM) across all your IT network devices? Yes No
2. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol across all your IT network devices? Yes No
3. Network Dependency – after how long will your business suffer financial impact by a loss to your network?

 6 hours 12 hours 24 hours 48 hours
4. How long will it take to fully restore your critical systems?

 6 hours 12 hours 24 hours 48 hours
5. What are your recovery time objectives for fully restoring your critical systems?

 6 hours 12 hours 24 hours 48 hours
6. Do you run your CNC machinery on a Direct Numerical Control basis? Yes No

If yes:

7. Please provide details of the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.)

8. Does your manufacturing network run within any unsupported operating systems (e.g. Windows XP)? Yes No
 - a. If you are operating on unsupported platforms, are these applications completely isolated from other platforms (e.g. air-gapped)? Yes No
9. Are any of your servers running manufacturing processes internet facing? Yes No
10. Are any of these servers managed by a supplier, and
 - a. If yes, does that supplier have a direct access to any of these servers? Yes No
11. Do you employ application white-listing? Yes No
12. Do you allow remote access to your manufacturing network only via 2 factor authentication? Yes No
13. Are critical patches applied within 30 days in your manufacturing environment? Yes No

GO TO DECLARATION

Financial Institutions

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

1. How many records of Personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process?

 0-50,000 50,000 - 100,000 100,000 - 250,000 250,000 - 500,000 500,000 - 1,000,000 1,000,000 +

2. 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

3. Have you deployed the following security protocols
 - I. Sender Policy Framework (SPF) and or
 - II. Domain Keys Identified Mail (DKIM) across all your devices?

 Yes No

4. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol??

 Yes No

5. Is all Personal data encrypted whilst in transit, backed up and at rest on the network?

 Yes No

6. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP) applicable to your business?

 Yes No

7. Is your critical data backed up, stored offline in an environment which is separate to your network and tested at least every 30 days for integrity?

 Yes No

8. Do you configure your network to provide high availability or failover for your website, critical applications and data you access / rely on to reduce any potential business interruption / downtime?

 Yes No

9. Have you successfully tested the restoration of (i.e. free from malware and no delay / unexpected downtime) your business critical applications and recovery of key server configurations in the last 12 months?

 Yes No

[GO TO DECLARATION](#)

Power Generation and Utilities

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

1. Have you deployed the following security protocols
 - I. Sender Policy Framework (SPF) and or
 - II. Domain Keys Identified Mail (DKIM) across all your IT network devices? Yes No
2. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol across all your IT network devices? Yes No
3. Network Dependency – after how long will your business suffer financial impact by a loss to your network?

 6 hours 12 hours 24 hours 48 hours
4. How long will it take to fully restore your critical systems?

 6 hours 12 hours 24 hours 48 hours
5. What are your recovery time objectives for fully restoring your critical systems?

 6 hours 12 hours 24 hours 48 hours
6. Do you run your CNC machinery on a Direct Numerical Control basis? Yes No

If yes:

7. Please provide details of the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.)

8. Does your manufacturing network run within any unsupported operating systems (e.g. Windows XP)? Yes No
 - a. If you are operating on unsupported platforms, are these applications completely isolated from other platforms (e.g. air-gapped)? Yes No
9. Are any of your servers running manufacturing processes internet facing? Yes No
10. Are any of these servers managed by a supplier, and
 - a. If yes, does that supplier have a direct access to any of these servers? Yes No
11. Do you employ application white-listing? Yes No
12. Do you allow remote access to your manufacturing network only via 2 factor authentication? Yes No

[GO TO DECLARATION](#)

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

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

1. How many records of Personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process?

| | | | | |
|--|--|--|---|--|
| <input type="checkbox"/> 0 - 10,000 | <input type="checkbox"/> 10,000 - 25,000 | <input type="checkbox"/> 25,000 - 50,000 | <input type="checkbox"/> 50,000 - 100,000 | <input type="checkbox"/> 100,000 - 250,000 |
| <input type="checkbox"/> 250,000 - 500,000 | <input type="checkbox"/> 500,000 - 1,000,000 | <input type="checkbox"/> 1,000,000 + | | |

2. Have you deployed the following security protocols

| | | |
|---|------------------------------|-----------------------------|
| I. Sender Policy Framework (SPF) and or | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| II. Domain Keys Identified Mail (DKIM) across all your devices? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

3. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

4. 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?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

5. Is all Personal data encrypted whilst in transit, backed up and at rest on your network?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

6. Is your critical data backed up, stored offline in an environment which is separate to your network and tested at least every 30 days for integrity?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

7. Do you comply with the current national and international legislation governing the handling of Personal data (e.g. GDPR, APP) applicable to your business?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

8. Do you configure your network to provide high availability or failover for your website, critical applications and data you access / rely on to reduce any potential business interruption / downtime?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

[GO TO DECLARATION](#)

Education

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

1. How many records of Personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process?

| | | | | |
|--|--|--|---|--|
| <input type="checkbox"/> 0 - 10,000 | <input type="checkbox"/> 10,000 - 25,000 | <input type="checkbox"/> 25,000 - 50,000 | <input type="checkbox"/> 50,000 - 100,000 | <input type="checkbox"/> 100,000 - 250,000 |
| <input type="checkbox"/> 250,000 - 500,000 | <input type="checkbox"/> 500,000 - 1,000,000 | <input type="checkbox"/> 1,000,000 + | | |

2. Is there a single policy governing all individual departments to control network and data security run by one department / provider?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

3. 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?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

4. Have you deployed the following security protocols

| | | | |
|-----|---|------------------------------|-----------------------------|
| I. | Sender Policy Framework (SPF) and or | | |
| II. | Domain Keys Identified Mail (DKIM) across all your devices? | | |
| | | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

5. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

6. Is all Personal data encrypted whilst in transit, backed up and at rest on your network?

7. Is your critical data backed up, stored offline in an environment which is separate to your network and tested at least every 30 days for integrity?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

8. 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?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

[GO TO DECLARATION](#)

Healthcare Centres and Professions

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

1. How many records of Personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process?
 0 - 10,000 10,000 - 25,000 25,000 - 50,000 50,000 - 100,000 100,000 - 250,000
 250,000 - 500,000 500,000 - 1,000,000 1,000,000 +
2. 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
3. Have you deployed the following security protocols
I. Sender Policy Framework (SPF) and or
II. Domain Keys Identified Mail (DKIM) across all your devices? Yes No
4. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol? Yes No
5. Is all Personal Data encrypted whilst in transit, backed up and at rest on your network?
6. Is your critical data backed up, stored offline in an environment which is separate to your network and tested at least every 30 days for integrity? Yes No
7. 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

[GO TO DECLARATION](#)

Technology and Telecommunications

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

1. How many records of Personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process?

| | | | | |
|--|--|--|---|--|
| <input type="checkbox"/> 0 - 10,000 | <input type="checkbox"/> 10,000 - 25,000 | <input type="checkbox"/> 25,000 - 50,000 | <input type="checkbox"/> 50,000 - 100,000 | <input type="checkbox"/> 100,000 - 250,000 |
| <input type="checkbox"/> 250,000 - 500,000 | <input type="checkbox"/> 500,000 - 1,000,000 | <input type="checkbox"/> 1,000,000 + | | |

2. Have you deployed the following security protocols

| | | |
|---|------------------------------|-----------------------------|
| I. Sender Policy Framework (SPF) and or | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| II. Domain Keys Identified Mail (DKIM) across all your devices? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

3. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

4. Is all Personal data encrypted whilst in transit, backed up and at rest on your network?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

5. Is your critical data backed up, stored offline in an environment which is separate to your network and tested at least every 30 days for integrity?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

6. Do you comply with the current national and international legislation governing the handling of Personal data (e.g. GDPR, APP) applicable to your business?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

7. Do you configure your network to provide high availability or failover for your website, critical applications and data you access / rely on?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

8. Are administrative privileges restricted to specific users on your computer network and only accessed by MFA?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

9. Have you successfully tested the restoration of (e.g. free from malware and no delay / unexpected downtime) your business critical applications and recovery of key server configurations in the last 6 months?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

10. Do you have contractual (indemnity) arrangements as an Outsource / Cloud provider / data processor with your customers for storing their Personal data in the event of a breach of privacy legislation by you?

| | | |
|--|------------------------------|-----------------------------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|--|------------------------------|-----------------------------|

If yes:

How much is the value range of the indemnity offered per client?

How many clients have an indemnity been issued to?

What is the average indemnity issued to a client?

GO TO DECLARATION

Wholesaling, Online Retailing, Transport, Logistics, Warehousing

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

1. What percentage of your revenue is delivered from online sales?
2. Do you have a business continuity plan that has a cyber-attack response procedure? Yes No
3. Do you test this business continuity plan annually? Yes No
4. Have you successfully tested the restoration of (e.g. free from malware and no delay / unexpected downtime) your business critical applications and recovery of key server configurations in the last 12 months? Yes No
5. Network Dependency – after how long will your business suffer financial impact by a loss to your network?
 6 hours 12 hours 24 hours 48 hours
6. How long will it take to fully restore your critical systems?
 6 hours 12 hours 24 hours 48 hours
7. What are your recovery time objectives for fully restoring your critical systems ?
 6 hours 12 hours 24 hours 48 hours
8. Do you (or your cloud service provider) configure your network to provide high availability or failover for your website and other critical applications? Yes No
9. Do you back up data that is necessary to run your business at least every 5 days? Yes No
10. Have you deployed the following security protocols
 - I. Sender Policy Framework (SPF) and or
 - II. Domain Keys Identified Mail (DKIM) across all your devices? Yes No
11. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol? Yes No

[GO TO DECLARATION](#)

Legal Professionals

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

1. How many records of Personal data on individuals (PCI, PII, PFI and / or PHI) do you collect, store and process?

| | | | | |
|--|--|--|---|--|
| <input type="checkbox"/> 0 - 10,000 | <input type="checkbox"/> 10,000 - 25,000 | <input type="checkbox"/> 25,000 - 50,000 | <input type="checkbox"/> 50,000 - 100,000 | <input type="checkbox"/> 100,000 - 250,000 |
| <input type="checkbox"/> 250,000 - 500,000 | <input type="checkbox"/> 500,000 - 1,000,000 | <input type="checkbox"/> 1,000,000 + | | |

2. 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?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

3. Have you deployed the following security protocols

| | | |
|---|------------------------------|-----------------------------|
| I. Sender Policy Framework (SPF) and or | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| II. Domain Keys Identified Mail (DKIM) across all your devices? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

4. If yes to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

5. Is your critical data backed up, stored offline in an environment which is separate to your network and tested at least every 30 days for integrity?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

6. Is all Personal data encrypted whilst in transit, backed up and at rest on your network?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

7. 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?

| | |
|------------------------------|-----------------------------|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No |
|------------------------------|-----------------------------|

[GO TO DECLARATION](#)

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





NSW

Suite 3, Level 18
201 Kent St
Sydney, NSW 2000

The Forum, Level 3
240 Pacific Highway
Charlestown, NSW 2290

QLD

Suite 1, Level 22
325 Queen St
Brisbane, QLD 4000

WA

PO Box 864
Joondalup, WA 6919