

OPTIONAL COVER(S)

Reputational Harm (Contingent Business Interruption)

Yes No

Limits: \$250,000 \$500,000 \$1,000,000

Tangible Property (Bricking) - \$25,000

Yes No

Cyber Crime

Yes No

If "yes" to Cyber Crime, please complete the following questions.

1. Limits: \$25,000 \$50,000 \$75,000 \$100,000 \$150,000

2. Can the Proposer confirm that the following operations are always segregated so that no individual person can control any operation from start to finish without referral to another person?

- a) Cheques being signed or payments being authorised above AUD\$10,000 Yes No
- b) Issuing funds transfer instructions Yes No
- c) Amending funds transfer procedures Yes No
- d) Opening new bank or supplier accounts Yes No
- e) Refund of monies or return of goods above AUD\$10,000 Yes No

3. Can the Proposer confirm that bank statements are always independently reconciled by persons who are not authorised to deposit and/or withdraw funds or issue funds transfer instructions? Yes No

4. Can the Proposer confirm whether an independent physical count of stock, raw materials, work in progress and finished goods is undertaken and whether the count is then reconciled against recorded stock levels? N/A Yes No

a) How frequently is a count undertaken?

b) Were there any discrepancies discovered during the most recent count? Yes No

If "Yes" to question 4b), please provide full details or attach an addendum:

5. Does the Firm have an approved suppliers list that is regularly updated and checked by the Directors or Officers? Yes No

6. Can the Proposer confirm that all suppliers, service providers and outsourcing companies are
- a) vetted for competency, financial stability and honesty before being approved? Yes No
 - b) appointed under a written contract? Yes No

If "No" to any part of question 7, please provide full details:

7. Does the proposer accept funds transfer instructions over the telephone, fax, email or some other electronic communications method?
 Yes No
8. Do employees receive anti-fraud training including but not limited to detection of impersonation fraud or phishing scams?
 Yes No N/A
9. Does the proposer verify any request to transfer funds made by an employee, officer or owners by calling back the employee, officer or owner at the telephone number listed in the company directory?
 Yes No N/A
10. Does the proposer have procedures in place to verify the authenticity of any payment or funds transfer request received by an employee from an internal company source (e.g. another employee, subsidiary, location or department)?
 Yes No N/A
11. Within the last three years, has the Firm discovered any employee dishonesty, burglary, robbery, disappearances, destruction or forgery losses?
 Yes No

If "Yes," please provide full details or attach an addendum:

12. Has the Firm ever been declined, had cancelled or non-renewed any insurance policy for Cyber Crime coverage?
 Yes No

If "Yes," please provide full details or attach an addendum:

I/We declare that the above answers, statements, particulars and additional information are true to the very best of the knowledge and belief of the Proposer. After full enquiry, I/We also confirm that I/We have disclosed all information and material facts that may alter the Underwriters' view of the risk, or affect their assessment of the exposures they are covering under the policy. I/We understand that all answers, statements, particulars and additional information supplied with this proposal form will become part of and form the basis of the policy.

I/We acknowledge that we have read and understood the content of the Important Notice contained in this proposal.

Signed:

Name in capital letters (printed):

Date:

Position:

For and/on behalf of the **Proposer**: