Cyber Insurance Proposal Form

Ocean Underwriting

Important Notices

Claims Made Insurance

The liability coverage provided under Ocean Underwriting Cyber Insurance policy is provided on a claims-made and notified basis. This means the policy provides cover for claims made against the insured and notified to the insurer during the policy period. This policy may not provide cover for any claims made against an insured, if at any time prior to commencement of this policy they were aware of facts which might give rise to those claims being made against them.

Section 40(3) of the *Insurance Contracts Act 1984* (Cth) provides that if an insured gives notice in writing to the insurer of facts that might give rise to a claim, as soon as reasonably practicable after becoming aware of such facts but before expiry of the policy period , then the insurer is not relieved of any liability under the contract in respect of the claim, if made, by reason only that it was made after the expiration of the policy period.

Duty of Disclosure

Ocean Underwriting Cyber Insurance policy is subject to the *Insurance Contracts Act 1984* (Cth), which imposes a duty of disclosure.

Before the insured enters into a contract of insurance, the insured has a duty to disclose anything that the insured knows, or could reasonably be expected to know, to be a matter relevant to the insurer's decision to enter into a contract of insurance with the insured and if so, on what terms.

The insured does not need to tell the insurer anything that:

- reduces the risk the insurer insures the insured for;
- is common knowledge;
- the insurer knows, or should know, as an insurer; or
- the insurer waives the insured's compliance with this duty.

The insured must comply with this duty up until the time the insurer agrees to insure the insured under a new contract of insurance or until an existing contract of insurance is renewed, varied, extended, reinstated or replaced.

Failure of the insured to comply with their duty of disclosure may entitle the insurer to cancel the policy or not accept a claim, in part or in full. If the insured's non-disclosure is fraudulent, the insurer may avoid the policy and treat it as if it never existed.

Insurer's privacy statement

The insurer is dedicated to upholding the insured's privacy and protecting their personal information, in a manner that meets Australian privacy laws, including the Privacy Act 1988 (Cth).

The insurer collects personal information when you deal with us, our agents, including the underwriting agent, and other companies in our global corporate group, as well as service providers which act on our behalf. The insurer uses your personal information so that it can conduct business with you. That includes the issuing and administration of this product, as well as the provision of related services, including claims handling and settling services.

The insurer may send your personal information overseas. The locations we may send it to can vary, but include Japan, USA, Canada, Bermuda, New Zealand, Thailand, Hong Kong, Europe (including the United Kingdom), Singapore and India. For more information about how the insurer handles your personal information or how to make a complaint about your privacy, please read the insurer's Privacy Policy, which is available online at tokiomarine.com.au or a free copy can be obtained by be emailing privacy@tokiomarine.com.au. The insurer's Privacy Policy is provided in Australia by its managing agent, Tokio Marine Management (Australasia) Pty Ltd.

It's up to you whether you provide your personal information to the insurer , however if you do not, the insurer might not be able to do business with you, and that could extend to not defending or paying a claim under the policy.

Ocean Underwriting's privacy statement

Within this privacy statement only, the underwriting agent is referred to as Ocean, 'We', 'Us' and 'Our'.

We use information provided by Our customers to allow Us to offer Our products and services. This means we may need to collect your personal information, and sometimes sensitive information about the insured as well (for example, your claims history). We will collect this information directly from the insured where possible, but there may be occasions when we collect this information from someone else. We will only use your information for the purposes for which it was collected, other related purposes and as permitted or required by law. The insured may choose not to give Us information, but this may affect Our ability to provide insurance cover. We may share this information with companies within Our group, government and law enforcement bodies if required by law and others who provide services to Us or on Our behalf, some of which may be located outside of Australia. By applying for, using or renewing any of Our products or services, or providing Us with your information, the insured agrees to this information being collected, held, used and disclosed as set out in this privacy statement. The insured can access Our privacy policy at: www.oceanunderwriting.com.au.

About the insurer

The insurer of this product is Tokio Marine & Nichido Fire Insurance Co., Ltd, ABN 80 000 438 291, AFS Licence No. 246548. In this document, the insurer is expressed as, 'we', 'us' and 'our'. Our managing agent and representative in Australia, Tokio Marine Management (Australasia) Pty Ltd, ABN 69 001 488 455 (TMMA), is authorised to act on our behalf, to issue this insurance product and handle and settle claims in relation to it.

About the underwriting agent

Ocean Underwriting Pty Limited, AFS Licence No. 542842, ABN 34 640 933 937, distributes and administers the Ocean Underwriting Cyber Insurance policy, as agent for the insurer. Ocean Underwriting acts as an agent for the insurer and not for the insured.

Notifications

All notifications and communications between the insured and the insurer under the Ocean Underwriting Cyber Insurance policy must be made through the underwriting agent, Ocean Underwriting Pty Limited.

Email:
hello@oceanunderwriting.com.au

Telephone:
(02) 9051 0708

Postal address:
Level 6, 60 Clarence Street Sydney NSW 2000

Incident response: 24-hour incident hotline

The insurer has a dedicated 24-hour emergency incident hotline, via its approved vendor that the insured must contact immediately following their discovery of any incident, circumstance, act, error or omission, that could reasonably result in a third party claim or first party loss.

Please refer to the policy schedule for the approved vendor's 24/7 contact details.

General Insurance Code of Practice

The General Insurance Code of Practice (Code) was developed by the Insurance Council of Australia to further raise standards of practice and service across the insurance industry. The Code Governance Committee (CGC) is an independent body that monitors and enforces insurers' compliance with the Code. The insurer has adopted and supports the Code and is committed to complying with it. For this product, the insurer complies with the Code to the extent it applies to wholesale insurance. Further information about the Code is available at www.codeofpractice.com.au or contact the insurer.

Important

Every question must be answered fully, truthfully and accurately.

- The information you provide in this document and through any other documentation, either directly or through your insurance broker, will be relied upon by the insurer to decide whether or not to accept your insurance as proposed and if so, on what terms.
- This Proposal Form will form part of any insurance under a policy issued upon the insurer's acceptance.
- If you do not understand or if you have any questions regarding any matter in this document please contact Ocean Underwriting or your insurance broker before signing the Declaration at the end of this document.

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. Signing this Proposal Form does not bind the applicant or the insurer to complete the insurance.

General Information

Details of Proposed Policyholder

FULL COMPANY/TRADING NAME

(including any subsidiaries to be included on the policy)

ADDRESS OF HEAD OFFICE

ABN

DATE ESTABLISHED

STATE OF REGISTRATION

BUSINESS ACTIVITY

Does your business partake in any of the below activities or professions:

- ☐ Payment processing
- ☐ Provide cloud services
- ☐ Peer to peer file sharing
- ☐ Third party claims administration
- ☐ Data hosting or aggregating
- ☐ Provide hotel/ accommodation services
- ☐ Manufacturer of life safety products or services
- ☐ Adult entertainment
- ☐ Online dating
- ☐ Firearms and weaponry services
- ☐ Defence contractor
- ☐ Credit bureau
- ☐ Cyber security products or services
- ☐ Trading exchanges
- ☐ Digital surveillance
- ☐ Social media platform provider
- ☐ Gambling
- ☐ Cryptocurrency exchange or distributed ledger technology
- ☐ Logistics for other companies

Website:

Is your business a franchisor? ☐ YES ☐ NO

Is your business a franchisee? ☐ YES ☐ NO

Revenue last financial year:

Revenue this financial year:

Stamp duty split:

Is there any overseas exposure? ☐ YES ☐ NO

If yes provide percentage revenue split in the box below:

COUNTRY	PERCENTAGE %
	0%
	0%
	0%
	0%
	0%
	0%

Is there any USA exposure? ☐ YES ☐ NO

Percentage of revenue made up from the United States of America:

Number of Employees:

Number of stored Personally Identifiable Information (PII) records:

Number of stored Protected Health Information (PHI) records:

Number of stored Payment Card Information (PCI) records:

Underwriting Questions

1. Are all computers in your organisation running Windows 10 or later? ☐ YES ☐ NO
2. Do you require passwords which meet minimum standards of complexity (8+ characters, utilising: uppercase letters, lowercase letters, numeric digits, and non-alphanumeric characters) and that are amended from vendor-supplied or default passwords? ☐ YES ☐ NO
3. Do you have anti-virus software installed on all company laptops, desktops, and servers and these are updated regularly? ☐ YES ☐ NO
4. Do you install all security patches (all vendors e.g. Microsoft) within 30 days of release? ☐ YES ☐ NO
5. Do you scan all incoming emails for malicious attachments and/or links? ☐ YES ☐ NO
6. Do you allow remote access to your network? (e.g. employees working from home, Citrix, cloud-based applications etc)
   a. If yes, do you require multi-factor authentication (MFA) for all remote access connections? ☐ YES ☐ NO
7. Do you use cloud-based email services (e.g. Office 365/ Gmail etc/Microsoft Outlook)?
   a. If yes, have you enabled multi-factor authentication (MFA)? ☐ YES ☐ NO
8. Do you take regular back-ups (at least weekly) of all critical data and store the backups offline, or offsite, or in a fire-proof safe, or does your outsourced service provider meet this requirement on your behalf? ☐ YES ☐ NO
9. Have you taken measure to comply with all the privacy and network security regulations and compliance standards applicable to the regions in which you operate? ☐ YES ☐ NO
10. Is your IT network segmented (VLAN, Firewall, Airgap, DMZ, etc) from other franchisees, i.e. no lateral movement from their network onto yours? ☐ YES ☐ NO

If Revenue is over 5,000,000 please complete the below:

11. Are firewalls installed on all gateways and configured to block inbound connections by default? ☐ YES ☐ NO

12. Are access controls employed using the principle of least privilege? ☐ YES ☐ NO

13. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? ☐ YES ☐ NO

14. Do you encrypt all data at rest, in-transit and all portable devices which are used to store personal data? ☐ YES ☐ NO

15. Have you taken measures to ensure that your organisation's website and print content do not infringe on any trademarks or copyright? ☐ YES ☐ NO

If Revenue is over 10,000,000 please complete the below:

16. Do you require multi-factor authentication for all access to privileged accounts, for both on premise and remote access? ☐ YES ☐ NO

17. Have you disabled all Remote Desktop Protocol (RDP) ports? ☐ YES ☐ NO

If Revenue is over 25,000,000 please complete the below:

18. Is your organisation PCI-DSS 3.2.1 compliant? ☐ YES ☐ NO

19. Do you take card-present payment transactions? ☐ YES ☐ NO

20. If Yes, for all payment card transactions, are all point-of-sale devices point-to-point (E2EE) encrypted? ☐ YES ☐ NO

21. Do you utilise any next generation anti-virus or behavioural analysis including Endpoint Detection and Response (EDR)? ☐ YES ☐ NO
    If yes, please state which product used (e.g CrowdStrike Falcon, SentinelOne)?

22. Do all employees receive training on cyber security, phishing, data protection and privacy matters? ☐ YES ☐ NO

23. What % of your total sales revenue is attributable to e-commerce?

Operational Technology Exposure

(Includes manufacturing, mining and utility industry classes)

1. Do you allow remote access to your operational technology network?
   If yes, do you require multi-factor authentication (MFA) for all remote access connections? ☐ YES ☐ NO

2. Do you segregate your operational technology from your IT network? ☐ YES ☐ NO

3. If yes, which method is used:
   ☐ VLANs ☐ Firewall ☐ DMZ ☐ Data Diode
   ☐ Air Gap ☐ Other:

4. Are any business-critical functions carried out on end-of-life/legacy systems where security patches are no longer available?
   If yes, do you use one of the following controls to mitigate this:
   - ☐ Application whitelisting
   - ☐ Purchase additional software support services
   - ☐ Endpoint Detection and Response (EDR)
   - ☐ Segmented from the rest of your OT network
   - ☐ Segmented from the internet.

5. Do you have a removable device (e.g. USB) policy:
   - ☐ Automatically blocked from running on the operational technology network
   - ☐ Scanned for malicious software prior to running
   - ☐ No policy in place

PCI Questions (if over 500,000 PCI records stored)

1. Is your organisation PCI-DSS 3.2.1 compliant? ☐ YES ☐ NO

2. Is the payment card data stored on your network 100% tokenised? ☐ YES ☐ NO

3. Do you accept card-present transactions? ☐ YES ☐ NO
   If 'Yes', for all payment card transactions, are all point-of-sale devices point-to-point (E2EE) encrypted? ☐ YES ☐ NO

Additional Coverage Questions

Crime Coverage Section

1. Is approval by more than one employee required to initiate a transfer of funds? ☐ YES ☐ NO

2. Does your bank require two-factor authentication (e.g. call-back) for all electronic funds transfer requests? ☐ YES ☐ NO

3. Do all third-party requests for payment go through a two-factor verification process (e.g. email request followed by telephone call)? ☐ YES ☐ NO

4. Do all third-party requests for changes to payment details (e.g. payee bank account details) go through a two-factor verification process? ☐ YES ☐ NO

5. Do all employees with financial or accounting responsibilities at your company receive social engineering training? ☐ YES ☐ NO

6. Has any entity to be insured here under experienced a wire transfer, telecom fraud or phishing attack loss in the past five years? ☐ YES ☐ NO

   If Yes, please provide complete details, including cause of loss, financial costs incurred and information on any subsequent improvements in controls that have been implemented:

Limit required

☐ $25,000 ☐ $50,000 ☐ $100,000

☐ $150,000 ☐ $250,000

Directors and Officers Cyber Coverage Section

1. What is your company structure?

   ☐ Pty Ltd ☐ Public Unlisted ☐ Non-Profit

   ☐ Publicly listed ☐ Trust ☐ Partnership

   ☐ Sole trader

2. Does your company have any securities listed on the stock exchange or planning an initial public offering during the coming 12 months? ☐ YES ☐ NO

3. Have you partaken in any mergers or acquisitions during the previous 12 months or planning on any in the next 12 months? ☐ YES ☐ NO

4. Limit required

   ☐ $150,000 ☐ $250,000

Policy Limit Required

☐ $250,000 ☐ $500,000 ☐ $1,000,000

☐ $2,00,000 ☐ $2,500,000 ☐ $3,000,000

☐ $5,000,000 ☐ Other:

Preferred Excess:

Claims/Circumstances

1. Does the applicant or proposed insured (including any director, officer, or employee) have any knowledge of any fact, circumstances, event or transaction which may give rise to a claim, loss or obligation to provide notification under the proposed insurance? ☐ YES ☐ NO

2. During the past five (5) years, has the applicant or proposed insured:
   a) Received any claims or complaints with respect to privacy, data protection or network security breach or unauthorised disclosure of information? ☐ YES ☐ NO
   b) Been subject to any government or regulatory investigation or action regarding any alleged violation of privacy and/or data protection laws ☐ YES ☐ NO
   c) Notified any persons of a privacy violation and/or data breach incident? ☐ YES ☐ NO
   d) Received an extortion demand relating to your data and/or computer systems? ☐ YES ☐ NO
   e) Received a complaint or cease and desist demand alleging intellectual property infringement by or on behalf of the applicant or proposed insured? ☐ YES ☐ NO
   f) Experienced a network outage that resulted in a significant disruption (e.g. disruption over 4 hours) of your computer operations? ☐ YES ☐ NO

3. If 'yes' to any of the above, please provide details regarding such incidents including any repeat attacks and remediation work that has been undertaken as a result?

Declaration

1. I/We have read and understood the information set out in the Important Notices section and other information on pages 1 to 3 of this proposal form.
2. I/We declare that I/We have made the necessary inquiries into the accuracy of the information and responses given in this proposal. The statements and particulars given in this proposal are true and complete, and that no material facts have been omitted, misstated or suppressed.
3. I/We agree that this proposal form, together with any other material information supplied by me/us shall form the basis of any contract of insurance effected thereon. I/We agree that should any of the information given by me/us alter between the date of this proposal form and the inception date of the insurance to which this proposal relates, I/we will give immediate notice thereof to the insurer.
4. I/We confirm that I/we am/are authorised by the proposing company (and its partners/principals/directors if applicable) to complete this proposal form and to accept the quotation terms for this insurance on behalf of the company (and its partners/principals/directors if applicable).
5. I/We consent to the insurer and the underwriting agent collecting, using and disclosing personal information as set out in the privacy statements in Important Notices section of this proposal form.
6. If I/we have provided or will provide information to the insurer about any other individuals, I/we confirm that I/we am/are authorised to disclose the other individual's personal information to the insurer and the underwriting agent, and also to give the above consent on both my/our and their behalf.
7. I/We authorise the undersigned is/are authorised to act for and on behalf of all persons and/or entities who may be entitled to indemnity under any policy which may be issued pursuant to this proposal form and I/we complete this proposal form on their behalf.

NAME

TITLE

SIGNATURE

DATE

CLEAR

Ocean Underwriting Pty Limited, AFSL 542842, ABN 34 640 933 937, is the underwriting agent for this product, which is issued by the insurer, Tokio Marine & Nichido Fire Insurance Co., Ltd., ABN 80 000 438 291, AFSL 246548, which is authorised to conduct general insurance business in Australia. Ocean Underwriting acts as an agent for the insurer, not the insured.