PROPOSAL FORM – SHORT

emergence

cyber event protection

Only use this proposal form if all of the following apply:

- Your estimated revenue is ≤ $25m, and
- You've requested a policy limit ≤ $5m, and
- You haven't suffered a cyber loss, and
- You are not in the IT, internet or telecommunications industry.

Completing this form requires technical knowledge of your IT. Consult with your IT manager or head of cyber security as necessary.

GENERAL

Australian Business Number (ABN):

Name of policyholder:

Is the policyholder a subsidiary, franchisee or part of a larger group? ☐ Yes ☐ No
If Yes, please provide details:

Business activities:

Do you perform work for the defence industry or Federal Government or are you a member of the Defence Industry Security Program (DISP)? ☐ Yes ☐ No

Policyholder's principal address:

Website(s) or domain(s):

List all domains for 'smarter cyber' monitoring or confirm: Don't know / don't have a website, domain or business email: ☐

Please provide the contact details of the person who is responsible for cyber security:
Note: This information will be used to provide critical security updates on a needs basis and will not be used for marketing purposes.

Name	Title
Email	Mobile

Total number of employees:

FINANCIALS

Estimated revenue for the coming 12 month period by territory:

		Are you located in the territory?
Australia/NZ	$	☐ Yes ☐ No
EU/UK	$	☐ Yes ☐ No
USA	$	☐ Yes ☐ No
Rest of world	$	☐ Yes ☐ No
Total	$ 0	

What percentage of total revenue is from online or e-commerce activities? %

Stamp Duty

For calculating stamp duty, outline the breakdown of revenue (000's) or employee numbers by state/region:

NSW	VIC	QLD	WA	SA	TAS	NT	ACT	NZ	O/S

Is the policyholder stamp duty exempt? If Yes, please provide a copy of the exemption letter. ☐ Yes ☐ No

PROPOSAL FORM – SHORT

cyber event protection

emergence

GOVERNANCE

1. How frequently do you provide security awareness training to your employees?
   ☐ Annually ☐ Quarterly ☐ Monthly ☐ Not provided

ASSET SECURITY

2. Have you implemented a critical security patch management process for your IT systems? ☐ Yes ☐ No

   If Yes, how do you handle security patches?
   ☐ Manual updates, implemented within 30 days
   ☐ Manual updates, implemented within 90 days
   ☐ Manual updates, no time frame for implementation
   ☐ Devices are set to update software automatically (where available)

IDENTITY AND ACCESS MANAGEMENT

3. Is Multi-Factor Authentication (MFA*) required for all users to access the following systems/platforms/services?

All remote access to the network?	☐ Yes ☐ No
Web-based email?	☐ Yes ☐ No
Admin/privilege service accounts?	☐ Yes ☐ No
Cloud resources, including back ups?	☐ Yes ☐ No

*Note: To qualify as multi-factor authentication, the authentication mechanism needs to be knowledge (something the user and only the user knows) and possession (something the user and only the user has). That way the compromise of any single device will only compromise a single authentication factor.

RESILIENCY AND RECOVERY

4. How frequently do you take regular backups of critical data and systems?
   ☐ Daily ☐ Weekly ☐ Monthly ☐ Greater than monthly

5. Do you keep a copy of critical backups offline, segregated from and inaccessible to your network? ☐ Yes ☐ No

6. Is your backup environment: (tick all that apply)

In the cloud	☐ Yes ☐ No
On premises	☐ Yes ☐ No
At a secondary, offsite data centre	☐ Yes ☐ No
Encrypted	☐ Yes ☐ No
MFA protected	☐ Yes ☐ No
Using immutable technology	☐ Yes ☐ No

PRIOR CLAIMS AND CIRCUMSTANCES

7. After enquiry, within the past 5 years, are you aware of any losses, claims, circumstances, cyber events, privacy breaches, regulatory investigations, crime or social engineering incidents which have impacted, or could adversely impact your business or give rise to a claim under a cyber policy? ☐ Yes ☐ No

   Total impact, including all business interruption, remediation costs and other loss? $

   Date of loss: / /

   Please indicate the nature of the loss by ticking the appropriate box:

   ☐ Crime ☐ Data breach ☐ Denial of service
   ☐ Email compromise ☐ Hacking, malware ☐ Multimedia injury
   ☐ Ransomware ☐ Social engineering
   ☐ Other please describe:

PRIOR CLAIMS AND CIRCUMSTANCES CONTINUED

What remediation steps and controls were implemented after the loss? (Attach report if available)

8. Have you had any unforeseen down time to your website or IT network of more than 8 hours? ☐ Yes ☐ No

If Yes, provide details including duration, how resolved and any cost to you:

OPTIONAL COVER - NON-IT CONTINGENT BUSINESS INTERRUPTION AND SYSTEM FAILURE

9. Do you want Optional Cover for Non-IT Contingent Business Interruption and System Failure? ☐ Yes ☐ No

10. Tell us about your critical components, service providers and supplies.

- ☐ All critical components, services and supplies are readily available from multiple sources
- ☐ Substitutes can be available within 10 days
- ☐ Longer than 10 days for substitutes to be available
- ☐ Don't know
- ☐ Substituting components, services or supplies is not possible

OPTIONAL COVER - CRIMINAL FINANCIAL LOSS

11. Do you want Optional Cover for Criminal Financial Loss? ☐ Yes ☐ No

Includes cyber theft, telephone phreaking, identity-based theft, push payment theft and cryptojacking. Does not include socially engineered theft unless selected below.

12. Aggregate limit for Criminal Financial Loss

☐ $10,000 ☐ $25,000 ☐ $50,000 ☐ $75,000 ☐ $100,000 ☐ $150,000 ☐ $250,000 ☐ Other $

13. Excess applicable to Criminal Financial Loss only

☐ $0 ☐ $2,500 ☐ $5,000 ☐ $10,000 ☐ $15,000 ☐ $25,000 ☐ $50,000 ☐ $75,000 ☐ $100,000

☐ Other $

14. Do you want to include cover for socially engineered theft? ☐ Yes ☐ No

15. Sublimit for socially engineered theft

The sublimit for socially engineered theft is included within and cannot be greater than the aggregate limit for criminal financial loss. The excess for criminal financial loss applies to socially engineered theft as well.

☐ $5,000 ☐ $10,000 ☐ $15,000 ☐ $20,000 ☐ $30,000 ☐ $50,000
☐ $75,000 ☐ $100,000 ☐ $125,000 ☐ $150,000 ☐ $200,000 ☐ $250,000

16. Are all new payees, and changes to existing payees' banking details, double authenticated with the payee? ☐ Yes ☐ No

17. Do transfers > $10,000 require dual signature or supervisor / manager sign off? ☐ Yes ☐ No

OPTIONAL COVER - CRIMINAL FINANCIAL LOSS CONTINUED

18. After enquiry, have you within the past 5 years suffered a crime, fidelity or computer crime loss? ☐ Yes ☐ No
    If Yes, please provide details:

OPTIONAL COVER - D&O LIABILITY

19. Do you want Optional Cover for Directors & Officers Liability? ☐ Yes ☐ No
    D&O Liability is only available for unlisted companies.

20. Aggregate sublimit for D&O Liability ☐ $250,000 ☐ $500,000 ☐ $1,000,000
    The sublimit for D&O Liability is included within and cannot be greater than the policy aggregate limit.

21. Are you listed on any stock exchange, or are you planning an initial public offering or any subsequent offering during the coming 12 months? ☐ Yes ☐ No

22. Have you within the past 5 years had D&O or Management Liability (ML) insurance declined or cancelled, or are you aware, after enquiry, of any D&O or ML loss, claim, or circumstance which has or could impact you or your business or give rise to a D&O or ML claim? ☐ Yes ☐ No
    If Yes, please provide details:

OPTIONAL COVER - TANGIBLE PROPERTY

23. Do you want Optional Cover for Tangible Property? ☐ Yes ☐ No
    The Tangible Property sublimit forms part of and is not in addition to the limit for Section C - Cyber Event Response Costs.

OPTIONAL COVER - JOINT VENTURE AND CONSORTIUM COVER

24. Do you want Optional Cover for your liability from joint ventures or consortia? ☐ Yes ☐ No
    If Yes, provide the name(s) of the joint venture or consortium:

Note: You must also include your share of revenue from the JV or consortium for the coming 12 months in your estimated total revenue.

TRADING NAMES, SUBSIDIARIES AND AFFILIATES

25. If you wish to list trading names, please list them individually in the boxes provided below.

26. If you wish to list subsidiaries, please list them individually in the boxes provided below.

Note: Subsidiaries of the policyholder are automatically covered and do not require scheduling. Listing an entity here does not extend cover or affect cover in any way. This list is for your convenience only.

27. Do you require cover for affiliated companies? ☐ Yes ☐ No

If Yes, please list the affiliates and revenue below and tell us how you are affiliated and about the IT.

Note: Listing an entity here means you are submitting it to Emergence for consideration. Cover will only apply to those entities accepted by Emergence and scheduled on the policy. You must provide revenue estimates for each entity and include revenue from all affiliates for the coming 12 months in your total estimated revenue.

Affiliate 1: Revenue $

Nature of affiliation: ☐ Authorised rep ☐ Family business ☐ Franchisee ☐ Shared directorships ☐ Other:

Is this affiliate's IT fully separate and independent? ☐ Yes ☐ No

If not, please describe any shared IT:

Affiliate 2: Revenue $

Nature of affiliation: ☐ Authorised rep ☐ Family business ☐ Franchisee ☐ Shared directorships ☐ Other:

Is this affiliate's IT fully separate and independent? ☐ Yes ☐ No

If not, please describe any shared IT:

You can include here other information or facts you would like to bring to the underwriter's attention:

PLEASE SPECIFY YOUR PREFERRED EXCESS, INDEMNITY PERIOD AND AGGREGATE LIMIT

Excess

☐ $0 ☐ $2,500 ☐ $5,000 ☐ $10,000 ☐ $15,000 ☐ $25,000 ☐ $50,000 ☐ Other $

Section A indemnity period

☐ 30 days ☐ 60 days ☐ 90 days ☐ 180 days ☐ 365 days

Policy aggregate limit

☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐ $2,000,000 ☐ $3,000,000 ☐ $4,000,000

☐ $5,000,000 ☐ $10,000,000 ☐ Other $

DECLARATION

I/we acknowledge that:

1. I/we have read and understood the important information provided on the last page of this document in the important information section.
2. I/we are authorised by all those seeking insurance to make this proposal, and declare all information on this proposal and any attachment is true and correct.
3. I/we authorise the underwriter to give to, or obtain from, other insurers or any credit reference service, any information relating to insurance held by me/us or any claim in relation thereto.
4. I/we acknowledge that, where answers are provided in the proposal are not in my/our handwriting, I/we have checked and certify that the answers are true and correct.

Policyholder's signature: Date: / /

GLOSSARY

Admin/privilege service accounts

Admin/privileged accounts refer to user accounts that have elevated privileges.

Admin accounts can manage and maintain a system or network.

Privileged accounts are used for automated processes or by applications that require elevated privileges to perform a task.

AI/automated rules-based enforcement

AI/automated rules-based enforcement is a mechanism designed to enforce predefined rules within security systems. An automated rules-based system is actively monitoring and enforcing certain rules or conditions to respond to a security threat.

Application whitelisting

Application whitelisting allows only authorised and approved applications to run on a system or network.

Content control software

Content-control software, commonly referred to as an Internet filter, is software that restricts or controls the content a user is able to access and/or download via the Internet.

Domain

A domain name (often called a domain) is an easy-to-remember name that's associated with a physical IP address on the Internet. It's the unique name that appears after the @ symbol in email addresses, and after www. in web addresses. Examples of domain names include google.com and wikipedia.org.

E-commerce activities

E-commerce involves the sale of goods and services over the internet. For example, online retail stores, digital products (e-books, music) and online marketplaces (eBay, Amazon etc).

Encryption

Encryption is the process of converting information or data into code to prevent unauthorised use.

Encryption at rest refers to encrypting data when it is stored on a device or storage system.

Encryption in transit refers to encrypting data as it travels across a network or between systems.

End of Life technology (EOL)

EOL refers to a stage in the life cycle of a technology product where it is no longer developed, maintained or supported by the manufacturer.

Endpoint Detection and Response (EDR)

EDR technology focuses on the detection, investigation, and mitigation of suspicious activities on endpoints including computers, servers and other devices within a network. EDR can identify anomalies and identify potential security threats.

Endpoint Protection Platform (EPP)

EPP is designed to defend endpoints such as laptops, servers and other devices connected to a network from various forms of malicious activities including malware, ransomware, and other cyber threats.

Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS)

IDS and IPS are technologies designed to detect and respond to malicious activities or security incidents within a computer network. IDS is used to monitor a network or system and identify patterns or behaviours that may indicate unauthorised access. IPS goes a step further than IDS by automatically blocking detected threats.

Immutable technology

Immutable technology is a type of technology or system where data or code cannot be altered or modified once it is created or deployed.

Multi-Factor Authentication (MFA)

MFA is a mechanism that requires individuals to provide more than one form of identification to access an account or system. The additional forms of identification can include one-time codes or biometrics.

Next Generation Firewall (NGFW)

NGFW combines traditional firewall capabilities with advanced functionalities such as application awareness, intrusion prevention, user identity awareness and advanced threat detection.

Payment Card Industry (PCI) assessment

PCI assessment is a process designed to evaluate a companies handling of credit card transactions to ensure a company complies with the PCI security standards.

Security Information and Event Management (SIEM)

A SIEM system provides real time analysis of logs that are gathered from various sources such as servers and security applications. A SIEM system will analyse the logs and identify potential security incidents.

Security patch management process

A security patch management process involves applying patches or updates to software and systems at regular intervals to address vulnerabilities and protect against security threats.

emergence

It is important that you read and understand the following.

Claims made notice

Section B – Loss to Others of this policy is issued on a 'claims made and notified' basis. This means that Section B – loss to others responds to:

a. claims first made against you during the policy period and notified to us during the policy period, provided that you were not aware at any time prior to the commencement of the policy of circumstances which would have put a reasonable person in your position on notice that a claim may be made against him/her; and:

b. written notification of facts pursuant to Section 40(3) of the *Insurance Contracts Act 1984 (Cth)*. Effectively, the facts that you may decide to notify are those which might give rise to a claim against you even if a claim has not yet been made against you. Such notification must be given as soon as reasonably practicable after you become aware of the facts and prior to the expiry of the policy period. If you give written notification of facts the policy will respond even though a claim arising from those facts is not made against you until after the policy has expired. When the policy period expires, no new notification of facts can be made to us on the expired policy for a cyber event or multimedia injury first discovered or identified by you during the policy period.

Your duty of disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms. You have this duty until we agree to insure you. You have the same duty before you renew, replace, extend, vary, continue under similar insurance or reinstate an insurance policy. 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 waive your duty to tell us about.

If you do not tell us anything you are required to, 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 policy as if it never existed.

About Emergence Insurance Pty Ltd

Before you enter into an insurance contract, you have a duty to Emergence Insurance Pty Ltd (ABN 46 133 037 153, AFSL 329634) ('Emergence') acts under a binding authority given to it by the insurer to administer and issue policies, alterations and renewals. In all aspects of arranging this policy, Emergence acts as an agent for the insurer and not for you.

Contact details are:

Email: info@emergenceinsurance.com.au

Telephone: 1300 799 562

Postal address: GPO Box R748, Royal Exchange, Sydney, NSW 2001

Privacy

In this Privacy Notice the use of "we", "our" or "us" means the Insurer and Emergence, unless specified otherwise.

We are committed to protecting your privacy.

We are bound by the obligations of the *Privacy Act 1988* (Cth) and the Australian Privacy Principles. These set out basic standards relating to the collection, use, storage and disclosure of personal information.

We need to collect, use and disclose your personal information (which may include sensitive information) in order to consider your application for insurance and to provide the cover you have chosen, administer the insurance and assess any claim. You can choose not to provide us with some of the details or all of your personal information, but this may affect our ability to provide the cover, administer the insurance or assess a claim.

The primary purpose for our collection and use of your personal information is to enable us to provide insurance services to you.

We may collect personal information in a number of ways, including directly from you via our website or by telephone or email.

Personal information will be obtained from individuals directly where possible and practicable to do so. Sometimes it may be collected indirectly (e.g. from your insurance intermediary or co-insureds). If you provide personal information for another person you represent to us that:

– you have the authority from them to do so and it is as if they provided it to us;
– you have made them aware that you will or may provide their personal information to us, the types of third parties we may provide it to, the relevant purposes we and the third parties we disclose it to will use it for, and how they can access it. If it is sensitive information we rely on you to have obtained their consent on these matters. If you have not done or will not do either of these things, you must tell us before you provide the relevant information.

We may disclose the personal information we collect to third parties who assist us in providing the above services, such as related entities, distributors, agents, insurers, reinsurers and service providers. Some of these third parties may be located outside of Australia, including New Zealand, Philippines, Vietnam, Malaysia and United Kingdom. In all instances where personal information may be disclosed to third parties who may be located overseas, we will take reasonable measures to ensure that the overseas recipieçnt holds and uses your personal information in accordance with the consent provided by you and in accordance with our obligations under *The Privacy Act 1988 (Cth)*.

In dealing with us, you consent to us using and disclosing your personal information as set out in this statement. This consent remains valid unless you alter or revoke it by giving written notice to Emergence's Privacy Officer. However, should you choose to withdraw your consent, we may not be able to provide insurance services to you.

The Emergence Privacy Policy available at www.emergenceinsurance.com.au or by calling Emergence, sets out how:

– Emergence protects your personal information;
– you may access your personal information;
– you may correct your personal information held by us;
– you may complain about a breach of *The Privacy Act 1988 (Cth)* or Australian Privacy Principles and how Emergence will deal with such a complaint.

If you would like additional information about privacy or would like to obtain a copy of the Privacy Policy, please contact the Emergence Privacy Officer by:

Postal Address: GPO Box R748, Royal Exchange, Sydney NSW 2001
Phone: 1300 799 562
Email: privacyofficer@emergenceinsurance.com.au

You can download a copy of the Emergence Privacy Policy by visiting www.emergenceinsurance.com.au.