CYBER PROPOSAL FORM

emergence

corporate

Use this proposal form if:

- Your actual revenue is >$250m, and
- You are not in the IT, internet or telecommunications industry.

Completing this form requires IT knowledge.
Consult with your Head of Cyber Security (or equivalent) 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 complete question 72. on page 13.

Business activities:

Do you perform work for the Defence industry or Federal Government? ☐ Yes ☐ No
If yes, please complete question 73. on page 13.

Policyholder's principal address:

Website(s) or domain(s):
List all domains for 'smarter cyber' monitoring.

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	Job Title
Email	Mobile

Total number of employees:

FINANCIALS

Estimated revenue for the coming 12 month period by territory:

	Prior 12 Months (Actual)	Current 12 Months (Projected)	Are you located in the territory?
Australia/NZ	$	$	☐ Yes ☐ No
EU/UK	$	$	☐ Yes ☐ No
USA	$	$	☐ Yes ☐ No
Rest of world	$	$	☐ Yes ☐ No
Total	**$**	**$**	

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

DATA PROTECTION

1. Do you collect, process, hold or store data on behalf of any 3rd party? ☐ Yes ☐ No

2. Please state the total number of personally identifiable information (PII) records you hold (including PII records you hold on behalf of others).
Note: All categories of PII relating to the same individual (whether active or inactive) should only count as a single unique record.

3. If this is held across multiple databases, please state the largest number of PII records held within a singular database.

☐ Not applicable

4. Please select the type of records collected, processed, held or stored: (tick all that apply)

Customer information (e.g. name, address, email address, phone number etc.)	☐ Yes ☐ No
Payment card information	☐ Yes ☐ No
Identity information (e.g. drivers licence, tax file number, passport number etc.)	☐ Yes ☐ No
Banking or financial information	☐ Yes ☐ No
Medical or healthcare information	☐ Yes ☐ No
Trade secrets or intellectual property	☐ Yes ☐ No
Biometric data	☐ Yes ☐ No

If you ticked biometric data, please complete our *biometric supplamentary form*.

5. Do you limit access to PII based on your employees needs according to their positions? ☐ Yes ☐ No

6. Do you control/limit/monitor an employees' ability to remove data or information from the network/office? (examples include USB drive security). ☐ Yes ☐ No

7. Do you have the following policies in place? (tick all that apply)

☐ Privacy policy ☐ Cookies policy ☐ Data retention and data destruction policy
☐ Bring your own device policy that ensures data on portable devices is encrypted

If you ticked data retention and destruction policy:

a) Does it include regular purging of data that you are no longer required to hold? ☐ Yes ☐ No

b) When was it last reviewed?

/ /

8. Do you protect all personally identifiable information and other sensitive data through encryption while: (tick all that apply)

At rest	☐ Yes ☐ No
In transit	☐ Yes ☐ No
Backed up	☐ Yes ☐ No
Stored on portable devices	☐ Yes ☐ No
Stored with 3rd parties	☐ Yes ☐ No

9. Do you utilise a Data Loss Prevention (DLP) tool? ☐ Yes ☐ No

If yes, is the DLP tool configured to actively block policy violations? ☐ Yes ☐ No

DATA PROTECTION (CONTINUED)

10. Do you (or a third party on your behalf) process payment card information (PCI)? ☐ Yes ☐ No

If yes, please outline the payment processors:

a) PCI DSS compliance level ☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4 ☐ Non compliant

b) Estimated number of PCI transactions processed annually

GOVERNANCE

11. Please select the appropriate structure of your information and cyber security:

- ☐ Centralised (information/cyber security is a central function which oversees all business units/ subsidiaries)
- ☐ Decentralised (each business unit/subsidiary is responsible for their own information/cyber security)
- ☐ Federated/hybrid (business units/subsidiaries have day-to-day management, but information/ cyber security policies and standards are centralised)

12. Select the frequency of your reports to the board on the organisation's cyber risk profile

☐ Annually ☐ Quarterly ☐ Monthly ☐ Other, please specify:

13. When was your privacy policy last reviewed by external legal counsel or management?

/ /

14. Do you maintain any certified information security standards? (e.g. ISO27001) ☐ Yes ☐ No

If yes, please include (e.g. standard & certification date, expiration date, etc.)

15. Have you adopted any cyber security frameworks of baselines? (e.g. NIST, Essential Eight)

If yes, please include (e.g. standard & certification date, expiration date, etc.)

16. How frequently do you provide security awareness training to your employees?

☐ Annually ☐ Quarterly ☐ Monthly ☐ Not provided ☐ Other, please specify:

17. How frequently do you test your employees' security awareness through simulated phishing campaigns?

☐ Annually ☐ Quarterly ☐ Monthly ☐ Not provided ☐ Other, please specify:

Do you require those employees that fail to undergo additional training?

☐ Yes ☐ No ☐ Not applicable

18. Do you require employees that have access to personally identifiable information (PII) to undertake data protection training at least annually? ☐ Yes ☐ No

ASSET MANAGEMENT

19. Do you maintain an inventory of hardware assets?

☐ Yes, automated ☐ Yes, manual ☐ No

If yes, does it capture 100% of assets?

☐ Yes ☐ No, please specify:

20. Do you maintain an inventory of software assets?

☐ Yes, automated ☐ Yes, manual ☐ No

If yes, does it capture 100% of assets?

☐ Yes ☐ No, please specify:

21. What is your approach to Bring Your Own Device (BYOD)?

ASSET SECURITY

22. Have you implemented hardened baseline configuration for all devices and systems? ☐ Yes ☐ No

23. Which of the following security solutions have you deployed? Tick all that applies and outline the product/vendor:

Solution	Product/Vendor
☐ Intrusion Detection System (IDS)	
☐ Intrusion Prevention System (IPS)	
☐ Endpoint Protection Platform (EPP)	
☐ Endpoint Detection and Response (EDR)	
☐ Managed Detection and Response (MDR)	
☐ Network Detection and Response (NDR)	
☐ Extended Detection and Response (XDR)	
☐ Security Information and Event Monitoring (SIEM)	
☐ Security Orchestration, Automation, and Response (SOAR)	
☐ Application Isolation and Containment	
☐ Application Whitelisting	
☐ Content control software (Web/URL filtering)	

24. What percentage (%) of endpoints and servers have EDR, MDR or XDR deployed?

Endpoints Servers

If less than 100%, please specify reasons why?

Indicate if AI/automated rules-based enforcement has been enabled: ☐ Yes ☐ No

ASSET SECURITY (CONTINUED)

25. Are alerts from all endpoints, servers and network and security appliances (including the EDR, MDR or XDR) fed into the SIEM (or similar)?

☐ Not applicable ☐ Yes ☐ No ☐ Partial, please specify:

26. How long does the SIEM solution retain logs?

☐ > 180 days ☐ 90 - 180 days ☐ 30 - 90 days ☐ < 30 days, please specify:
☐ Not applicable

27. Do you have a Security Operations Centre (SOC)?

☐ Yes, 24/7 ☐ Yes, working hours only ☐ No

If yes, is it internally or externally managed?

☐ Internal ☐ External ☐ Both

28. How do you handle the security patch management process? (tick all that apply)

☐ Devices are set to update software automatically (where applicable)
☐ Manual updates, implemented within 30 days
☐ Manual updates, implemented based on vulnerability criticality. Please outline target timelines and compliance rates

Critical:		High:		Medium:		Low:	
Hours	%	Days	%	Days	%	Days	%

If your compliance rate is <95%, can you please provide some insights as to why and what mitigating measures you would implement in the event you cannot apply the patch in a timely fashion?

29. What risk-based network segmentation is in place to prevent lateral movement? (tick all that apply)

☐ Business unit ☐ Geography ☐ Isolation of critical systems
☐ Data storage based on sensitivity of data ☐ Other, please specify:

30. Do you have a Web Application Firewall (WAF) in front of all externally facing applications? ☐ Yes ☐ No

If yes, is it in blocking mode? ☐ Yes ☐ No

EMAIL SECURITY

31. Which of the following email security measures have been deployed? (tick all that apply)

☐ Email filtration and scanning tool to authenticate emails, flag and quarantine suspicious content (e.g. executable files)

EMAIL SECURITY (CONTINUED)

- ☐ Authentication of outbound emails through:
- ☐ Domain-based Message Authentication, Reporting and Conformance (DMARC)
- ☐ DomainKeys Identified Mail (DKIM)
- ☐ Sender Policy Framework (SPF)
- ☐ External emails are tagged
- ☐ Quarantine all suspicious emails
- ☐ Process for reporting suspicious email
- ☐ Sensitive external emails are sent securely
- ☐ Disable macros by default
- ☐ Investigation of email attachments in a sandbox

IDENTITY AND ACCESS MANAGEMENT

32. Please confirm if you enforce Multi-Factor Authentication (MFA) for all: (tick all that apply)
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.

a) Remote access to the network? If no, please specify reasons why. ☐ Yes ☐ No

b) Web-based and cloud-hosted email accounts? If no, please specify reasons why. ☐ Yes ☐ No

Please confirm this applies to all employees, contractors and outsource providers?
If no, please specify reasons why: ☐ Yes ☐ No

33. Do you use any remote desktop tools or software? (e.g. Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), AnyDesk, TeamViewer, or similar)

☐ Yes ☐ Yes, but internally only and not exposed to the internet ☐ No

If yes, is MFA enforced?

☐ Yes ☐ No, please specify reasons why:

IDENTITY AND ACCESS MANAGEMENT (CONTINUED)

34. How do you protect privilege accounts? (tick all that apply)

- ☐ MFA is enforced for all administrator/privileged accounts
- ☐ Administrators have unique privileged credentials, separate from their everyday user credentials, to perform administrative tasks
- ☐ Privileged access workstations are utilised
- ☐ Privilege access logs are retained for at least 90 days
- ☐ Privilege accounts are monitored for irregular activity
- ☐ Credentials are managed, secured and rotated using a password vault
- ☐ The just-in-time access (which is time bound) methodology is utilised
- ☐ Utilisation of a Privilege Access Management (PAM) or Privilege Identity Management (PIM) tool.

If yes, please specify which product:

35. How many do you have of the following:

a) Global admin accounts

b) Domain or other admin accounts

c) Privileged service accounts

Are they periodically reviewed? ☐ Yes ☐ No

36. Have you configured all service accounts to deny interactive logons?

☐ Yes ☐ No, please specify reasons why:

37. Do you allow ordinary users local administration rights?

☐ No ☐ Yes, please specify reasons why and how many users have these rights:

38. Do you provide ordinary users with password management software? ☐ Yes ☐ No

ASSESSMENTS

39. How frequently do you conduct vulnerability scans?

☐ Annually ☐ Bi-Annually ☐ Quarterly ☐ Monthly ☐ Other, please specify:

ASSESSMENTS

40. What percentage of your environment is covered by the vulnerability scans? %

41. How frequently do you engage an independent external provider to conduct penetration testing?

☐ Annually ☐ Bi-Annually ☐ Quarterly ☐ Monthly ☐ Other, please specify:

42. Have all critical and high severity recommendations within your latest penetration test been remediated?

☐ Yes ☐ No, please specify:

43. Do you use Breach and Attack Simulation (BAS) software?

☐ Yes ☐ No, please specify reasons why:

END OF LIFE TECHNOLOGY

44. Do you rely on any operating system, software or hardware that is no longer supported or is considered end of life by the manufacturer? ☐ Yes ☐ No

If Yes, please answer the following questions:

Is any end of life technology internet facing? ☐ Yes ☐ No

Is it segregated from the rest of the network? ☐ Yes ☐ No

Has additional support been purchased where available? ☐ Yes ☐ No

Please outline any additional security measures that have been implemented to prevent exploitation of any vulnerabilities:

RESILIENCY AND RECOVERY

45. How frequently do you take backups of critical data and systems?

☐ Daily ☐ Weekly ☐ Monthly ☐ Other, please specify:

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

47. Where do you store backups? (tick all that apply)

☐ Cloud ☐ Offline ☐ At a Secondary Data Centre ☐ In a separate segment of the network

RESILIENCY AND RECOVERY (CONTINUED)

48. Which of the following have you implemented to secure the backup environment? (tick all that apply)

☐ Encryption ☐ Vaulted Credentials ☐ Segmentation ☐ MFA ☐ Immutable

49. Do you use any commercial backup solutions (e.g. Commvault, Veeam etc.) ☐ Yes ☐ No

If yes, please outline which product is used:

50. How frequently do you test system restoration capabilities by performing a full restoration from a sample set of backup data?

☐ Monthly ☐ Quarterly ☐ Annually ☐ Other, please specify:

51. Do you have the ability to test the integrity of the backups to ensure they are free of malware prior to restoration? ☐ Yes ☐ No

52. Do you maintain an alternative backup IT facility?

☐ Cold site ☐ Warm site ☐ Hot site ☐ None

53. Do you have the capability to immediately failover to redundant or standby information systems? ☐ Yes ☐ No

54. Please describe the impact to your operations and revenue should you suffer an outage of the IT network of more than 72 hours.

55. Please confirm which of the following formal plans you have in place (which addresses cyber incidents) and whether tested at least annually:

	In place?	Tested annually?
Disaster Recovery Plan (DRP)	☐ Yes ☐ No	☐ Yes ☐ No
Business Continuity Plan (BCP)	☐ Yes ☐ No	☐ Yes ☐ No
Incident Response Plan (IRP)	☐ Yes ☐ No	☐ Yes ☐ No

Does your IRP specifically address ransomware scenarios? ☐ Yes ☐ No

56. Please outline what specific planning has been undertaken with respect to responding to a ransomware incident (e.g. a ransomware playbook, tabletop scenario with senior management etc.)

OUTSOURCE PROVIDERS

57. Do you rely on any outsource providers for any business-critical application or platforms?

☐ No ☐ Yes, please specify:

OUTSOURCE PROVIDERS (CONTINUED)

58. Do you require outsource providers to maintain cyber security controls and risk management which align with or exceed their own cyber security controls and risk management?

- ☐ Yes, all outsource providers
- ☐ Yes, however only critical IT Contractors and those that handle/hold PII
- ☐ No

59. Do you audit your outsource providers at least annually?

- ☐ Yes, all outsource providers
- ☐ Yes, however only critical IT Contractors and those that handle/hold PII
- ☐ No
- ☐ Other, please specify:

60. How frequently do you waive their rights of recourse against IT contractors for service interruptions?

☐ Never ☐ Rarely ☐ Some of the time ☐ Always

61. Please outline the your top 10 IT contractors:

IT Contractor Name	Services Provided
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

MEDIA LIABILITY

62. Do you publish any blogs, newsletters, videos, podcasts, or similar content? ☐ Yes ☐ No

If yes,

a) Do you seek legal review prior to publication of new content? ☐ Yes ☐ No

b) Does the content include intellectual property owned by third parties? ☐ Yes ☐ No

OPERATIONAL TECHNOLOGY

63. Do you use operational technology?

If yes, please complete *operational technology supplemental form*. ☐ Yes ☐ No

MERGERS AND ACQUISITIONS

64. Have you made any acquisitions in the last 5 years? Please include details (e.g. name, size of entity, business activities and date of acquisition).

65. Do you ensure the acquiree's computer systems, security controls and risk management are equal to or better than your own prior to acquisition? ☐ Yes ☐ No

    If no, please provide an overview of how this is handled? (e.g. do you use best endeavours within a reasonable period of time to either bring the computer systems and risk management to an equivalent standard or to ensure the computer systems will be absorbed promptly into your computer systems?)

66. Does your due diligence process include ascertaining if the acquiree has suffered any past cyber events? ☐ Yes ☐ No

SANCTIONS

67. Do you conduct business in or provide services to organisations or individuals within any territory which are subject to Australian, UN, UK, EU or US sanctions restrictions?

    ☐ No ☐ Yes, please specify:

68. Do you connect to any network, contract with, or rely on, any IT contractors, whether under the policyholders control or a third party, that is located within a territory subject to Australian, UN, UK, EU or US sanctions restrictions?

    ☐ No ☐ Yes, please specify:

PRIOR CLAIMS AND CIRCUMSTANCES

69. Within the last 5 years have you had a cyber insurance policy declined or cancelled? If yes, please provide details. ☐ Yes ☐ No

PRIOR CLAIMS AND CIRCUMSTANCES (CONTINUED)

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

a) 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

- ☐ Email compromise
- ☐ Ransomware
- ☐ Data breach
- ☐ Hacking, malware
- ☐ Denial of service
- ☐ Multimedia injury
- ☐ System failure
- ☐ Other

Please provide a detailed description:

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

71. 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:

SUBSIDIARY, FRANCHISEE OR PART OF A LARGER GROUP

72. Is the policyholder a subsidiary, franchisee or part of a larger group?
If you selected yes on page one, please provide additional details here..

i. Please select which type:

☐ subsidiary ☐ franchisor ☐ franchisee ☐ part of larger group

ii. What is the structure of the policyholder's IT network?

☐ Centralised (information/cyber security is a central function which oversees all business units/subsidiaries)
☐ Decentralised (each business unit/subsidiary is responsible for their own information/cyber security)
☐ Federated/hybrid (business units/subsidiaries have day-to-day management, but information/cyber security policies and standards are centralised)

iii. Does your parent company/franchisor purchase a cyber policy? ☐ Yes ☐ No
If yes, does their cyber policy include cover for the Policyholder? ☐ Yes ☐ No

DEFENCE OR FEDERAL GOVERNMENT WORK

73. Do you perform work for the Defence industry or Federal Government?
If you selected yes, on page one, please provide additional details here.

i. Please select which type: ☐ defence ☐ federal government

ii. What percentage of your revenue is derived from Defence industry or Federal Government contracts?

Defence % Federal Government %

iii. What is the nature of the work performed?

iv. Do you hold a DISP membership or have AGSVA security clearance? ☐ Yes ☐ No
If yes, please outline which level:

DECLARATION

I/we acknowledge that:

1. Have read and understood the important information provided on the last page of this document in the important information section.
2. 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. 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. 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: / /

emergence

It is important that you read and understand the following.

Claims made notice

Section B – Cyber & Privacy Liability and Section E – Optional Cover – multimedia liability of this policy is issued on a 'claims made and notified' basis. This means that Section B – Cyber & Privacy Liability and Section E – Optional Cover – multimedia liability 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

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

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 recipient 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 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