Cyber Enterprise Solution Proposal Form

emergence

General

1. Name of policyholder:

2. Business activities:

3. Australian Business Number (ABN):

4. Is the policyholder a subsidiary, franchisee or smaller company of a larger group? ☐ Yes ☐ No
If yes, please provide details.

5. Policyholder's principal address (Suburb, State, Postcode):

6. Website(s):

7. 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	Phone	Email

8. Total number of employees:

Financials

1. Please provide the following revenue (AUD) derived from each region:

	Past Calendar Year (Actual)	Current Calendar Year (Projected)
A/NZ	$	$
EU/UK	$	$
USA	$	$
Rest of World	$	$
Total Revenue	$ 0	$ 0

2. What percentage (%) of total revenue is from online or e-commerce activities? %

3. Please indicate your annual IT budget: $

4. Please indicate what percentage (%) of your IT budget is attributed to cyber security: %

Stamp Duty

1. For the purpose of calculating stamp duty, please outline the percentage (%) breakdown of revenue or employee numbers by state/region:

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

2. Is the policyholder Stamp Duty exempt? *If yes, please provide a copy of the exemption letter.*

☐ Yes ☐ No

Governance

1. Please select the appropriate structure of the policyholder's 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)

2. Select the frequency the policyholder reports to the board on the organisation's cyber risk profile

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

3. When was the policyholders formal privacy policy last reviewed by legal and management?

/ /

4. Does the policyholder maintain any certified information security standards? (e.g., ISO27001)

☐ Yes ☐ No

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

5. Has the policyholder adopted any cyber security frameworks or baselines? (e.g., NIST, Essential Eight etc)

☐ Yes ☐ No

If yes, please include details (e.g., maturity level etc)

6. How frequently does the policyholder provide security awareness training to their employees?

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

7. How frequently does the policyholder test their employees' security awareness through simulated phishing campaigns?

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

Does the policyholder require those employees that fail to undergo additional training?

☐ Yes ☐ No ☐ Not applicable

8. Does the policyholder require employees that have access to personally identifiable information (PII) to undertake data protection training at least annually?

☐ Yes ☐ No

Cyber Enterprise Solution Proposal Form

emergence

Asset Management

1. Does the policyholder maintain an inventory of hardware assets?
   ☐ Yes, automated ☐ Yes, manual ☐ No

   If yes, does it capture 100% of assets?
   ☐ Yes ☐ No, please specify:

2. Does the policyholder maintain an inventory of software assets?
   ☐ Yes, automated ☐ Yes, manual ☐ No

   If yes, does it capture 100% of assets?
   ☐ Yes ☐ No, please specify:

3. What is the policyholder's approach to Bring Your Own Device (BYOD)?

Asset Security

1. Has the policyholder implemented hardened baseline configuration for all devices and systems?
   ☐ Yes ☐ No

2. Which of the following security solutions has the policyholder deployed? *Select 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)	

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

   If less than 100%, please specify reasons why?

4. 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:

Asset Security continued

5. How long does the SIEM solution retain logs?

☐ > 180 days ☐ 90 – 180 days ☐ 30 – 90 days ☐ < 30 days, please specify:

☐ Not applicable

6. Does the policyholder 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

7. Please outline the target timelines within your patch management process and compliance rates (%) with those target timelines over the last 12 months:

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

8. What mitigating measures does the policyholder take in the event a patch cannot be implemented in a timely fashion?

9. What risk-based network segmentation is in place to prevent lateral movement? *Select all that apply.*

☐ Business unit ☐ Geography ☐ Isolation of critical systems

☐ Data storage based on sensitivity of data ☐ Other, please specify:

10. Does the policyholder 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

1. Which of the following email security measures have been deployed? *Select all that apply:*

☐ Scans and filter inbound emails for malicious content (e.g., executable files)

☐ 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

1. Please confirm the Policyholder enforces Multi-Factor Authentication (MFA) for all:

   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?

   ☐ Yes ☐ No, please specify reasons why:

   b) Web-based and cloud-hosted email accounts?

   ☐ Yes ☐ No, please specify reasons why:

   Please confirm this applies to all employees, contractors and outsource providers?

   ☐ Yes ☐ No, please specify:

2. 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:

3. Please select which of the following applies with respect to protection of privilege credentials:

   ☐ 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:

Identity and Access Management continued

4. How many does the Policyholder have of the following:

   a) Global admin accounts

   b) Domain or other admin accounts

   c) Privileged service accounts

   Are they periodically reviewed?

   ☐ Yes ☐ No

5. Has the policyholder configured all service accounts to deny interactive logons?

   ☐ Yes ☐ No, please specify reasons why:

6. Does the policyholder allow ordinary users local administration rights?

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

7. Does the policyholder provide ordinary users with password management software?

   ☐ Yes ☐ No

Assessments

1. How frequently does the policyholder conduct vulnerability scans?

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

2. What percentage of the Policyholders environment is covered by the vulnerability scans?

   %

3. How frequently does the Policyholder engage an independent external provider to conduct penetration testing?

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

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

   ☐ Yes ☐ No, please specify:

5. Does the policyholder use Breach and Attack Simulation (BAS) software?

   ☐ Yes ☐ No

Data Protection

1. Please state the total number of personally identifiable information (PII) records held by the policyholder. *Note: all categories of PII relating to the same individual (whether active or inactive) should only count as a single unique record.*

Data Protection continued

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

☐ Not applicable

3. Please select the type of PII records held.
   - ☐ Basic customer information (e.g., name, address, email address, phone etc)
   - ☐ Payment card information
   - ☐ Personal Identity Information (e.g., drivers licence, tax file numbers, passport number etc)
   - ☐ Banking or financial
   - ☐ Medical or healthcare data

4. Does the policyholder limit access to PII based on their employees needs according to their position?
   ☐ Yes ☐ No

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

6. Does the policyholder have a data retention and destruction policy?
   ☐ Yes ☐ No If yes,
   a) Does it include regular purging of data that the policyholder is no longer required to hold.
   ☐ Yes ☐ No
   b) When was it last reviewed?
   / /

7. Please indicate when PII is encrypted:
   ☐ At rest ☐ In Transit ☐ Stored on portable devices ☐ While backed up

8. Does the policyholder utilise a Data Loss Prevention (DLP) tool?
   ☐ Yes ☐ No
   If yes, is the DLP tool configured to actively block policy violations?
   ☐ Yes ☐ No

9. Does the policyholder (or a third party on behalf of the policyholder) 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 ☐ Not Compliant
   b) Estimated number of PCI transactions process annually

10. Does/has the policyholder collect, transmit, receive or retain biometric information of employees or customers? *If yes, please complete biometric supplemental form.*
    ☐ Yes ☐ No

End of Life Technology

1. Does the policyholder rely on any operating systems, 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:

   a) Are they segregated from the rest of the network?

   ☐ Yes ☐ No

   b) Additional support has been purchased where available

   ☐ Yes ☐ No

   c) Please outline any additional security measures that have been implemented to prevent exploitation of any vulnerabilities.

Resiliency and Recovery

1. How frequently does the policyholder take regular backups of critical data and systems?

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

2. Does the policyholder keep a copy of critical backups offline, segregated from and inaccessible to your network?

   ☐ Yes ☐ No

3. Where does the policyholder store backups? Select all that apply.

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

4. Which of the following has the policyholder implemented to secure the backup environment? Select all that apply.

   ☐ Encryption ☐ Vaulted Credentials ☐ Segmentation ☐ Multi-factor Authentication ☐ Immutable

5. Does the policyholder use any commercial backup solutions (e.g., Commvault, Veeam etc)

   ☐ Yes ☐ No

   If yes, please outline which product is used:

6. How frequently does the policyholder test system restoration capabilities by performing a full restoration from a sample set of backup data?

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

7. Does the policyholder have the ability to test the integrity of the backups to ensure they are free of malware prior to restoration?

   ☐ Yes ☐ No

8. Does the policyholder maintain an alternative backup IT facility?

   ☐ Cold site ☐ Warm site ☐ Hot site ☐ None

9. Does the policyholder have the capability to immediately failover to redundant or standby information systems?

   ☐ Yes ☐ No

Resiliency and Recovery continued

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

11. Please confirm which of the following formal plans the policyholder has, are in place (which addresses cyber incidents) and are tested at least annually?

	In Place	Tested at least annually
a) Disaster Recovery Plan (DRP)	☐	☐
b) Business Continuity Plan (BCP)	☐	☐
c) Incident Response Plan (IRP)	☐	☐

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

Outsource Providers

1. Does the policyholder rely on any outsource providers for any business-critical applications or platforms?
   ☐ Yes ☐ No, please specify:

2. Does the policyholder 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

3. Does the policyholder audit their 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:

4. How frequently does the policyholder waive their rights of recourse against IT contractors for service interruptions?
   ☐ Never ☐ Rarely ☐ Some of the time ☐ Always

Outsource Providers continued

5. Please outline the policyholders top 10 IT contractors:

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

Media Liability

1. Does the policyholder publish any blogs, newsletters, videos, podcasts or similar content?

   ☐ Yes ☐ No

   If yes,

   a) Does the policyholder 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

1. Does the policyholder use operational technology? *If yes, please complete operational technology supplemental form.*

   ☐ Yes ☐ No

Mergers and Acquisitions

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

Mergers and Acquisitions continued

2. Does the policyholder ensure the acquiree's computer systems, security controls and risk management are equal to or better than their own prior to acquisition?

☐ Yes ☐ No

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

3. Does the policyholder's due diligence process include ascertaining if the acquiree has suffered any past cyber events?

☐ Yes ☐ No

Sanctions

1. Does the policyholder 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:

2. Does the policyholder 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

1. Within the past 5 years has the policyholder:

a) Had a cyber insurance policy declined or cancelled? If yes, please provide details.

☐ No ☐ Yes

Prior Claims and Circumstances continued

b) Suffered a cyber event which has impacted their business?

☐ No ☐ Yes, please provide a description of the cyber event including date of the occurrence, type of incident, financial impact and remedial action taken to prevent a reoccurrence:

c) Received any demands or claims relating to allegations of theft of information, breach of information security or network security?

☐ No ☐ Yes, please provide details:

d) Been the subject of any regulatory investigation, government action of any kind, or been served with a subpoena regarding any alleged or failure to comply with any privacy/data security law or regulation?

☐ No ☐ Yes, please provide details:

2. After enquiry, is the policyholder aware of any facts, circumstances or cyber events that could give rise to a claim under a cyber policy?

☐ No ☐ Yes, please provide details:

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.

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.

Name:
Title:
Date:
Signature:

Important Information

emergence

It is important that you read and understand the following:

Claims made notice

Section C – Cyber & Privacy Liability and Section F – Optional Cover – Multimedia Liability Cover of this policy are issued on a 'claims made and notified' basis. This means that Section C – Cyber & Privacy Liability and Section F – Optional Cover – Multimedia Liability Cover respond to:

1. Claims or multimedia claims first made against you during the policy period and notified to us during the policy period, provided 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 or multimedia claim may be made against you; and
2. written notifications 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 or multimedia claim against you even if a claim or multimedia claim has not yet been made against you. If you decide to notify any such facts, 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 to any claim or multimedia claim against you arising from those facts, even if the claim or multimedia claim 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 under 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, 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 policy 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 327 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 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.

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 coinsureds).

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. 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.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 327 Sydney, NSW 2001
Phone: 1300 799 562
Fax: +61 2 9307 6699
Email: privacyofficer@emergenceinsurance.com.au

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