CHUBB®

Cyber ERM Mid-Market

Proposal Form

Completing the Proposal Form

- Please read the "Statutory Notice" before completing this proposal form.
- If you have insufficient space to complete any of your answers, please attach a separate signed and dated sheet and identify the question number concerned.
- It is agreed that whenever used in this proposal form, the term Applicant shall mean the Organisation and all its Subsidiaries and the definition of the terms 'Claims', 'Policy Period', 'Defence Costs', 'Director' or 'Officer' are in accordance with the policy.
- The cyber liability insuring clause of the Cyber ERM policy is written on a claims made basis and only claims first made during the policy period or any extended reporting period.
- The limit of liability to pay damages or settlements will be reduced and may be exhausted by the payment of defence costs, or legal representation expenses.

A. General Applicant Information	
1. Name of Applicant:	
2. Applicant's address:	
3. Web site address:	
4. Nature of Applicant's activities:	
5. How long has the Applicant continuously carried on business?	
6. Names and dates under which the Applicant's business was formerly carried on:	

B. General Risk Information	
General Information	
1. Does the Applicant anticipate in the next twelve (12) months establishing or entering into any related or unrelated ventures which are a material change in operations? If yes, please provide full details on a separate sheet.	☐ Yes ☐ No

2. Please complete the following information for the Applicant:

	Prior year	Current year	Projected year
a) Number of Employees			
b) Total Assets			
c) Gross Revenues			
d) Gross Revenue from on-line sales or service			

3. How many servers does the Applicant either own or otherwise have dedicated to their use?	
4. What is the Applicant's total number of IP addresses?	☐ Yes ☐ No
5. Does the Applicant collect, store or process personally identifiable or other confidential information?	☐ Yes ☐ No
If yes, how many records are held, including the Applicant's prospective, current and former customers and employees?	

6. Does the Applicant comply with privacy and data protection legislation applicable to all jurisdictions and industry standards, in which it operates? (e.g. Australian Privacy Principles, HIPAA Privacy Rules, EU Data Protection Regulations).	☐ Yes ■ No
7. Does the Applicant process or store personally identifiable or other confidential information forthird parties? If yes, please attach an explanation.	☐ Yes ☐ No
8. Does the Applicant shred all written or printed personally identifiable or other confidentialinformation when it is being discarded?	☐ Yes ☐ No
PCI Compliance	
1. The Applicant subject to Payment Card Industry (PCI) Security Standards? If yes, please complete question 2 and 3. If no, continue to the next section.	☐ Yes ☐ No
2. How many credit or debit card transactions does the Applicant process annually?	
3. Does the Applicant:	
a) Mask all but the last four digits of a card number when displaying or printing cardholder data?	☐ Yes ☐ No
b) Ensure that card-validation codes are not stored in any of the Applicant's databases,log files or anywhere else within their network?	☐ Yes ☐ No
c) Encrypt all account information on the Applicant's databases?	☐ Yes ☐ No
d) Encrypt or use tokenisation for all account information at the point of sale?	☐ Yes ☐ No
Information Security Policies	
1. Has the Applicant implemented a formal information security policy which is applicable to all ofthe Applicant's business units? If yes;	
a) Does the Applicant test the security required by the security policy at least once annually?	☐ Yes ☐ No
b) Does the Applicant regularly identify and assess new threats and adjust the security policy to address new threats?	☐ Yes ☐ No
c) Does the Applicant's information security policy include policies for the use and storage of personally identifiable or other confidential information on laptops?	☐ Yes ☐ No
Web Server Security	
1. Does the Applicant store personally identifiable or other confidential information on theirweb servers?	☐ Yes ☐ No
2. Do the Applicant's web servers have direct access to personally identifiable or otherconfidential information?	☐ Yes ☐ No
3. Does the Applicant have firewalls that filter both inbound and outbound traffic?	☐ Yes ☐ No
Virus Protection, Intrusion Detection & Penetration Testing	
1. Are anti-virus programs installed on all of the Applicant's PC's and network systems? If yes, how frequently are the virus detection signatures updated?	☐ Yes ☐ No
2. Does the Applicant employ intrusion detection or intrusion protection devices on their network, or IDS or IPS software on the Applicant's hosts?	☐ Yes ☐ No
If yes, how frequently are logs reviewed?	
3. Does the Applicant run penetration tests against all parts of their network?	☐ Yes ☐ No
If yes, how often are the tests run?	
4. Has the Applicant been the target of any computer or network attacks (including virus attacks) in the past two (2) years?	☐ Yes ☐ No
If yes, did the number of attacks increase?	
Mobile Device Security	
1. Does the Applicant store personally identifiable or other confidential information on mobile devices?	☐ Yes ☐ No
If yes, does the Applicant encrypt such information?	☐ Yes ☐ No

Business Continuity	
1. Does the Applicant have a Business Continuity Plan (BCP) specifically designed to address a network related denial-of-service attack? If yes;	☐ Yes ☐ No
a) Is the BCP reviewed and updated at least bi-annually?	☐ Yes ☐ No
b) Is the BCP tested at least once annually?	☐ Yes ☐ No
c) Have any problems identified during testing been rectified?	☐ Yes ☐ No
d) Does your BCP address the destruction of or corruption of your applications and data?	☐ Yes ☐ No
If yes to question 1 d),	
i) What is the estimated cost of restoring applications or data and the cost of recovery?	
ii) How long do you think it would take to restore applications and/or data?	

Security Assessments	
1. Has an external system security assessment, other than vulnerability scans or penetration tests been conducted within the past twelve (12) months?	☐ Yes ☐ No
If yes, please indicate who conducted the assessment, attach copies of the result, and indicate whether all critical recommendations have been corrected or complied with:	
If no, please attach an explanation.	

Backup & Archiving	
1. How frequently does the Applicant back up electronic data?	
2. Where does the Applicant store back up electronic data?	
3. Does the Applicant store back up electronic data with a third party service provider?	☐ Yes ☐ No

Service Providers	
1. Does the Applicant use vendors that provide you with infrastructure, platform, software orstorage services?	☐ Yes ☐ No
If yes, for all vendors that provide the Applicant with infrastructure, platform, software or storage services, do you:	
a) Require that they comply with specific security requirements?	☐ Yes ☐ No
b) Assess and confirm that they meet your required levels of security?	☐ Yes ☐ No
c) Have the requisite security procedures and requirements written into the contract with them?	☐ Yes ☐ No
d) Require that they indemnify you for damages you sustain because they failed to implement or maintain your required level of security?	☐ Yes ☐ No
e) Require that they provide insurance for damages that you sustain?	☐ Yes ☐ No

Incident Response Plans	
1. Does the Applicant have a formal incident response plan that addresses network security incidents or threats?	☐ Yes ☐ No

C. Security Incident and Loss History:

1. Has the Applicant ever had any computer or network security incidents? "Incident" includes any unauthorised access to any computer, system, database or data, intrusion or attack, the denial of use of any computer or system, intentional disruption, corruption or destruction of electronic data, programs or applications or any other incidents similar to the foregoing?	☐ Yes ☐ No
If yes, please describe in the text box below:	
a) The magnitude of the attack(s) including how long each attack lasted and the average pps rate; and	
b) What actions you took to mitigate or recover from it and the cost of carrying out those mitigation/recovery actions.	

2. Have any loss payments been made on behalf of any Applicant or any person proposed for coverage under any cyber security policy or similar insurance?	☐ Yes ☐ No
3. In the past five (5) years has anyone intentionally damaged or corrupted, or attempted to damage or corrupt your applications or data? If yes, please describe in the text box below:	☐ Yes ☐ No
a) Whether the perpetrator was employed by you and, if so, whether they were an employee or contractor;	
b) How the perpetrator got access to the applications or data; and	
c) What actions you took to recover the applications or data and the cost of the recovery.	

D. Stamp Duty

1. Please state the total number of employees located in the following states and overseas:

NSW	VIC	ACT	QLD	SA	WA	TAS	NT	O/S

2. GST	
a) Applicant's Australian Business Number:	
b) Does the Applicant intend to claim an Input Tax Credit for the premium of the proposed policy if provided?	☐ Yes ☐ No
If yes, to what extent is an Input Tax Credit being claimed by any and which Applicants (e.g. full claim or %)?	

E. Declaration and Signature

The undersigned authorised officers of the Applicant declare that to the best of their knowledge and belief the statements set forth herein and all attachments and schedules hereto are true and immediate notice will be given should any of the above information alter between the date of this proposal and the proposed date of inception of the insurance. Although the signing of the proposal does not bind the undersigned, on behalf of the Applicant, to effect insurance, the undersigned agree that this proposal and all attachments and schedules hereto and the said statements herein shall be the basis of and will be incorporated in the policy should one be issued.

The undersigned, on behalf of the Applicant, acknowledge that the Statutory Notice contained herein has been read and understood.

This proposal must be signed by the Applicant's Chairman of the Board, Managing Director or Chief Executive Director.

Date:		Signed:	
Title:			

Privacy Statement

Chubb Insurance Australia Limited (Chubb) is committed to protecting your privacy. This document provides you with an overview of how we handle your personal information. Our Privacy Policy can be accessed on our website at www.chubb.com/au.

Personal Information Handling Practices

Collection, Use and Disclosure

We collect your personal information (which may include sensitive information) when you are applying for, changing or renewing an insurance policy with us or when we are processing a claim in order to help us properly administrate your insurance proposal, policy or claim.

Personal information may be obtained by us directly from you or via a third party such as your insurance intermediary or employer (e.g. in the case of a group insurance policy).

When information is provided to us via a third party we use that information on the basis that you have consented or would reasonably expect us to collect your personal information in this way and we take reasonable steps to ensure that you have been made aware of how we handle your personal information.

The primary purpose for our collection and use of your personal information is to enable us to provide insurance services to you. Sometimes, we may use your personal information for our marketing campaigns, in relation to new products, services or information that may be of interest to you. We may disclose the information we collect to third parties, including service providers engaged by us to carry out certain business activities on our behalf (such as assessors and call centres in Australia). In some circumstances, in order to provide our services to you, we may need to transfer personal information to other entities within the Chubb Group of companies (such as the regional head offices of Chubb located in Singapore, UK or USA), or third parties with whom we or those other Chubb Group entities have sub-contracted to provide a specific service for us, which may be located outside of Australia (such as in the Philippines or USA). Please note that no personal information is disclosed by us to any overseas entity for marketing purposes.

In all instances where personal information may be disclosed overseas, in addition to any local data privacy laws, we have measures in place to ensure that those parties hold and use that information in accordance with the consent you have provided and in accordance with our obligations to you under the Privacy Act 1988 (Cth)

Your Choices

In dealing with us, you agree to us using and disclosing your personal information as set out in this statement and our Privacy Policy. This consent remains valid unless you alter or revoke it by giving written notice to our Privacy Officer. However, should you choose to withdraw your consent it is important for you to understand that this may mean we may not be able to provide you or your organisation with insurance or to respond to any claim.

How to Contact Us

If you would like a copy of your personal information, or to correct or update it, please contact our customer relations team on 1800 815 675 or email CustomerService.AUNZ@chubb.com.

If you have a complaint or would like more information about how we manage your personal information, please review our Privacy Policy for more details or contact the Privacy Officer: Chubb Insurance Australia Limited, GPO Box 4907, Sydney NSW 2001, O +61 2 9335 3200, E Privacy.AU@chubb.com.

Statutory Notice

A. 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 or reinstate an insurance contract.

What you do not need to tell us

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 something

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 contract as if it never existed.

B. Subrogation

You may prejudice your rights with regard to a claim if, without prior agreement from the Insurer, you make agreement with a third party that will prevent the Insurer from recovering the loss from that, or another party.

Your policy contains provisions that either exclude the Insurer from liability, or reduce their liability, if you have entered into any agreements that exclude your rights to recover damages from another party in relation to any loss, damage or destruction which would allow you to sustain a claim under this policy.

Other Important Information

C. Utmost Good Faith

Every insurance contract is subject to the doctrine of utmost good faith which requires that parties to the contract should act toward each other with the utmost good faith. Failure to do so on your part may prejudice any claim or the continuation of cover provided by the Insurer.

D. Not a Renewable Contract

Cover under this policy will terminate at expiry of the Period of Insurance specified in your policy document. If you wish to effect similar insurance for a subsequent period, it will be necessary for you to complete a new proposal form prior to the termination of the current policy so that terms of insurance and quotation/s can then be developed for your consideration.

E. Change of Risk or Circumstances

It is vital that you should advise us of any departure from your “normal” form of business (i.e. that which has already been conveyed to the Insurer). For example, acquisitions, changes in location or new overseas activities.

About Chubb in Australia

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for over 50 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages include Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, for a broad client base, including many of the country's largest companies.

More information can be found at www.chubb.com/au

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Chubb. Insured.[SM]