QBE Australia Cyber Response
Cyber and Data Security Insurance Application

QBE Insurance (Australia) Limited ABN 78 003 191 035 AFSL 239 545

You must read this notice before you complete the proposal form.

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.

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.

Claims made

This Policy operates on a 'claims made and notified' basis. This means that the Policy covers you for claims made against you and notified to us during the period of insurance.

The Policy does not provide cover in relation to:
1. acts, errors or omissions actually or allegedly committed prior to the retroactive date of the Policy (if such a date is specified);
2. claims made after the expiry of the period of insurance even though the event giving rise to the claim may have occurred during the period of insurance;
3. claims notified or arising out of facts or circumstances notified (or which ought reasonably to have been notified) under any previous policy;
4. claims made, threatened or intimated against you prior to the commencement of the period of insurance;
5. facts or circumstances of which you first became aware prior to the period of insurance, and which you knew or ought reasonably to have known had the potential to give rise to a claim under this Policy; and
6. claims arising out of circumstances noted on the proposal form for the current period of insurance or on any previous proposal form.

Where you give notice in writing to us of any facts that might give rise to a claim against you as soon as reasonably practical after you become aware of those facts but before the expiry of the period of insurance, you may have rights under section 40(3) of the *Insurance Contracts Act 1984 (Cth)* to be indemnified in respect of any claim subsequently made against you arising from those facts notwithstanding that the claim is made after the expiry of the period of insurance. Any such rights arise under the legislation only. The terms of the Policy and the effect of the Policy is that you are not covered for claims made against you after the expiry of the period of insurance.

Privacy

Our Privacy Policy describes how we collect, disclose, store and use personal information as well as how to access it, correct it or make a complaint. We use personal information to issue, administer and manage products and provide services. You can view our Privacy Policy at www.qbe.com.au/privacy, or to obtain a free copy phone us on 133 723 or ask one of our authorised representatives or service providers.

We may share personal information with other QBE Group companies, our authorised representatives and service providers, each of which may be based outside of Australia.

By giving us personal information you consent to us collecting, disclosing, storing and using it in accordance with our Privacy Policy. If you give us someone else's personal information you confirm you've obtained their consent to do so.

If you don't provide all of the personal information we've requested, we may be unable to issue, administer or manage products or provide services.

QBE Australia Cyber Response
Cyber and Data Security Insurance Application

QBE Insurance (Australia) Limited ABN 78 003 191 035 AFSL 239 545

IMPORTANT: Please answer ALL questions fully. If there is insufficient space please provide details on your letterhead.
Where provided, tick (✓) appropriate box to indicate answer.

1. Company Information

Company Name			
Address			
		Post Code	
ABN			
Number of employees		Business Establishment Date	

Please provide a description of your business services? (and note if there has been any changes to business activities or any mergers and acquisitions in the last 12 months):

		Previous	Current	Next Year
Please provide turnover for the following financial years	$A			
Please provide profit for the following financial years (net profit before tax)	$A			

Stamp Duty Split

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

Please list any Overseas countries if noted above

2. IT Structure

1. Service Providers

Service	**Service Provider**
Internet Service Provider	
Cloud / Hosting Provider (Including backup and storage providers)	
Payment Processing	
Data or Information Processing	
IT Security	
Other (please specify)	

1.i For any of the above vendor arrangements, does this involve the transfer any Personally Identifiable Information records to third-parties outside Australia? Yes ☐ No ☐

1.ii If so, do you ensure that the countries in which these third-parties hold your Personally Identifiable Information records have government legislation and regulation on data protection? Yes ☐ No ☐ N/A ☐

1.iii Do you have a written contract in place with the third party vendors noted above that will indemnify you for IT system or data security breaches arising from their services? Yes ☐ No ☐

1.IV As part of your third party vendor engagements, do you ensure contracts contain a right of audit of vendor security systems, and also allow a full review of the vendors security systems in place prior to engagement? Yes ☐ No ☐

1.V As part of your third party vendor engagements, do you ensure any contracts contain a provision whereby all security incidents are to be reported to you? Yes ☐ No ☐

2.i Please estimate the following;

- Number of servers	
- Number of server locations for your business.	
- Number of PC's	
2.ii Please provide a financial value for your IT network (including but not limited to hardware, software, cabling and firmware)?	$

3.i Please estimate the total number of Personally Identifiable Information records, including employees and customers that your company holds?

3.ii If applicable, what proportion of the Personally Identifiable Information records are of USA/Canada clients? %

3.iii Please estimate what proportion of the total number of Personally Identifiable Information records you hold include a highly sensitive element?: %

(e.g banking account numbers, debit card numbers, credit card numbers, medical information, legal information, corporate confidential information)

3.iv Do you see any of these changing substantially in the next 12 months? Yes ☐ No ☐

If yes, please provide details

3.v Please tick the type of Personally Identifiable Information stored (*tick below*);

Low Sensitivity		Moderate Sensitivity		High Sensitivity	
Name	☐	Home address	☐	Banking or Saving Account number	☐
E-mail address	☐	Telephone numbers	☐	Debit Card number	☐
		Insurance Policy number	☐	Credit Card number	☐
		Date of birth	☐	Health information	☐
		Drivers License number	☐	Legal information	☐
		Passport number	☐		

4. Where you have outsourced credit card data / transactions to a payment processor, have they confirmed they are PCI compliant? Yes ☐ No ☐ N/A ☐

5. Do you sell / share confidential information (Including Personal Identifiable Information) with any third parties? Sell ☐ Share ☐ N/A ☐

3. IT Security

Baseline Security

1. Do you use an automatically updating anti-virus and anti-spyware system to protect your network and business applications? Yes ☐ No ☐

2. Do you ensure that all personally identifiable information records and business critical information is backed up and held at a secondary location? If yes, please tick how frequently below backups are created? Daily ☐ Weekly ☐ >Monthly ☐

3. Do you have firewalls protecting your internal and external IT Networks? Yes ☐ No ☐

Prevention

1. Do you have a policy in place which ensures updates and critical security patches for all IT and business applications are installed in a timely manner (if not automatic, within 30 days of being released)? Yes ☐ No ☐

2. Are all core business systems (Operating Software / Internet Browser / Anti-virus / Business Applications) updated to latest version, or do you ensure that the current versions are still being serviced and maintained by the developer? Yes ☐ No ☐

3. Do you engage in application whitelisting on your internal network? Yes ☐ No ☐

4. Do you ensure that administrative network and system credentials are only given to appropriate staff members based on their role? Yes ☐ No ☐

5. Have you had a third party security audit or penetration test undertaken on your IT network in the last 12 months? Yes ☐ No ☐

5.i If yes, have you implemented the recommendations of the audit? Yes ☐ No ☐

If no, please provide details

6. Do you have physical controls and registration for visitors at your company's entrance area? Yes ☐ No ☐

7. Are all Personally Identifiable Information records, including those contained in a physical form (paper, disks, CD's, hard drives), disposed of or recycled by a confidential and secure means which is recognised throughout the organisation? Yes ☐ No ☐

8. Are systems that collect, store and transfer sensitive data segregated from the main network? Yes ☐ No ☐

Detection

1. Do you have a vulnerable assessment program that monitors for network and data security breaches and anomalies (including security logs being created and aggregated in a centralised source)? Yes ☐ No ☐

2. Does the above incorporate monitoring of logs with the ability to issue automatic security alerts based on defined variables and thresholds? Yes ☐ No ☐

Response

1.i Do you have a disaster recovery plan (DRP) in place for all critical systems which ensures you can continue to operate during and after a sudden or unexpected failure to your IT network and/or a security breach/data compromise? Yes ☐ No ☐

1.ii Is any DRP back-up system managed by a Third Party? Yes ☐ No ☐

1.iii How regularly are DRP's tested/updated? <12 Months ☐ > 12 Months ☐

1.iv When was it last tested?

1.v How long did it take to switch to this back-up system?

2. How fast are you likely to incur a loss of profit as a result of an IT network compromise and a total system downtime? (Tick Below)

Level 1: 48 Hours + ☐ **Level 2:** 24-48 hours ☐ **Level 3:** 12-24 hours ☐

Level 4: 1-12 hours ☐ **Level 5:** Immediately ☐

3. In the event of your IT network being subjected to a non-scheduled closure and total downtime; please estimate your maximum daily loss of profit (net profit before tax)? $

Culture/Compliance

1. Do you have a Chief Information Officer (CIO), Chief Security Officer (CSO), or any other executive responsible for data security and compliance? Yes ☐ No ☐

2. Do you have a staff member whose sole responsibility is IT security? Yes ☐ No ☐

3. Do you have an internal Legal department? Yes ☐ No ☐

4. Do you have an Internal Public Relations department? Yes ☐ No ☐

5. Have you identified, and are compliant, with all regulatory and industry supported compliance frameworks that are applicable to your organisation? Yes ☐ No ☐

6. Do you adhere to and comply with the following (tick below):

	Yes	No	Not Applicable
Privacy Act 1988 including the Australian Privacy Principles	☐	☐	☐
Office of the Australian Information Commissioner Regulations and Guidelines	☐	☐	☐
ISO 27001:2013 Information and Data Security	☐	☐	☐
Payment Card Industry (PCI) Data Security Standards	☐	☐	☐

If PCI standards are applicable to your business, please tick merchant level below

1 ☐ 2 ☐ 3 ☐ 4 ☐

6.i Please estimate the annual number of processed credit card transactions

6.ii Do you store credit card Primary Access Numbers (PAN) on your network? Yes ☐ No ☐

6.iii If yes to the above, do you ensure you comply with the PCI DSS Requirements for protecting cardholder data? Yes ☐ No ☐

7.i Do you have an internet and email usage policy written into all employment contracts which is clearly communicated to all employees? Yes ☐ No ☐

7.ii If yes, does this permit the monitoring and investigation of computer activity of your employees? Yes ☐ No ☐

8. Do you implement a data protection policy for the handling of data including Personally Identifiable Information records which is clearly communicated to all employees? Yes ☐ No ☐

9. Do you use encryption tools to ensure the integrity and confidentiality of the below (please tick)?

	Yes	No
Portable media	☐	☐
Data in transit	☐	☐
Data at rest	☐	☐
Backup data	☐	☐
Business critical or confidential data	☐	☐

10. When recruiting new employees to you undertake thorough background checks before employment is offered? Such as: Police Record Checks, Identity, Qualifications, Disciplinary? Yes ☐ No ☐

11. Upon termination of employment, do you ensure all log-in and system access credentials access are revoked within 3 days of termination? Yes ☐ No ☐

4. Website

Website	

1. Do any of your websites contain any of the following (tick if applicable)?

Financial transactions via payment cards ☐

Storage/ input of medical records or private information of individuals ☐

Storage/ input of legal advice or services ☐

Streaming of music or video ☐

Social network functionality ☐

2. Please confirm the approximate % of income derived from website activities? %

3. Do you have a privacy policy on your website? Yes ☐ No ☐

4. Do you have a specific policy for managing all 'opt-in' / 'opt-out' marketing requests including the use/storage of cookies on a browsers system/device? Yes ☐ No ☐

5. Do you have a procedure for responding to allegations that content created, displayed or published is libellous, infringing intellectual property rights, or in violation of a third party's privacy right? Yes ☐ No ☐

6. If applicable, please describe what procedures you have in place for monitoring or moderating content posted on your website including your "take-down" policy?

7. Do you obtain written warranties and indemnities from third parties for content they have created for you (including advertising agents)? Yes ☐ No ☐

5. Limits required

Cover and Quotation requirements

Please indicate which sections of cover you require an Indicator for: Please tick where appropriate.

Cyber, data security and multimedia cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$1,000,000 ☐ $2,000,000 ☐ $5,000,000 ☐ $10,000,000 ☐

Data breach notification costs cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$1,000,000 ☐ $2,000,000 ☐ $5,000,000 ☐ $10,000,000 ☐

Information and communication asset rectification costs cover

Limit of indemnity is subject to the value of your IT network (as per IT Structure questions 2.Ii)

Regulatory defence and penalty costs cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$100,000 ☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐

Public relations costs cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$100,000 ☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐

Forensics costs cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$100,000 ☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐

Credit monitoring costs cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$100,000 ☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐

Cyber business interruption cover

Limit of Indemnity is subject to your net profit before tax.

Cyber extortion cover

Please select Limit of Indemnity each and every occurrence and in the aggregate:

$1,000,000 ☐ $2,000,000 ☐ $5,000,000 ☐ $10,000,000 ☐

Excess

$

Please note that the policy is subject to a Total Aggregate Limit of Indemnity. Please refer to the policy terms and conditions for further information. Please ask your broker for a copy of the policy wording.

6. Claims

If yes to 2-3 below, please provide further information on a separate document.

1. Have you previously been insured in respect of Cyber and Data Security? Yes ☐ No ☐

2. Has your business ever been declined for a Cyber and Data Security insurance policy, or had an existing policy cancelled? Yes ☐ No ☐

3. Have you ever experienced an event that did or would have given rise to a claim or circumstance under a cyber and data security policy, including but not limited to hacking incident, virus or malicious code attach, cyber extortion attempt, breach of secure data, wrongful disclosure of personal data or interference with rights of privacy? (if "yes", please provide further information on the event below)? Yes ☐ No ☐

4. Please provide details of any matter which may be relevant to insurers consideration of your proposal and which has not been disclosed elsewhere in this proposal.

7. Declaration and authorisation

Please remember we will treat a statement or claim or act or omission by any one of the applicants as a statement or claim or act or omission by all of the applicants

- I/We have received a copy of the Policy Terms and Conditions
- I/We declare that this proposal has been completed after appropriate enquiry and that the statements and particulars in this proposal (including all attachments, if applicable) are true and that I/We have neither misrepresented or suppressed any material facts.
- I/We undertake to inform Insurers of any material alteration to these facts whether occurring before or after the completion of the contract of insurance.
- I/We authorise QBE Insurance (Australia) Limited ABN 78 003 191 035 to give or obtain from other insurers or insurance reference bureaus or credit reporting agencies, any information about this insurance or any other insurance held by the business including this completed application and the business's claims history and credit history.

Applicant/Intermediary's signature Date (dd/mm/yyyy)

Please return the completed form to your financial services provider.

This Policy is underwritten by QBE Insurance (Australia) Limited ABN 78 003 191 035