Cyber Event Protection

Proposal

Important notice

- This is a proposal for a contract of insurance, in which 'Proposer' or 'you/your' means the individual, company, partnership, limited liability partnership, organisation or association proposing cover. 'Ando' or 'we/us/our' means Ando Insurance Group Limited.
- This proposal must be completed, signed and dated. All questions must be answered to enable a quotation to be given but completion does not bind you or Ando to enter into any contract of insurance. If space is insufficient to answer any questions fully, please attach a signed continuation sheet. You should retain a copy of the completed proposal (and of any other supporting information) for future reference.
- All facts material to the proposed insurance must be disclosed, fully and truthfully to the best of your knowledge and belief. Failure to do so may make the contract of insurance voidable and Ando may treat it as having no effect and never having existed, or severely prejudice your rights in the event of a claim. A material fact is one likely to influence Underwriters' assessment or acceptance of the proposal; if you are uncertain what may be a material fact, you should consult your broker.
- You are recommended to request a specimen copy of the proposed policy wording from your insurance broker and to consider carefully the terms, conditions, limitations and exclusions applicable to the cover.

Broker details

Broker company name			
First name		Last name	
Mobile		Work phone	
Email address			

Proposer contact details

First name		Last name	
Mobile		Work phone	
Email address			
Role			

Company details

Company name/ Trading as	
Business description	
Website	

Company Address

Suburb | Town/City | Postcode

Postal address (if different from company address)

Suburb | Town/City | Postcode

Please provide your estimated revenue for the coming 12 month period by region, and indicate in which territories you are located.

Region	Revenue	In which territories are you located?		
New Zealand/Australia	$	New Zealand/Australia	Yes	No
EU/UK	$	EU/UK	Yes	No
USA	$	USA	Yes	No
Rest of World	$	Rest of World	Yes	No
Total Revenue	$			

Please specify your preferred excess, indemnity period and aggregate limit

Excess
- $1,000
- $2,500
- $5,000
- $10,000
- $15,000
- $25,000
- Other (please specify) _____

For Section A Indemnity Period
- 30 days
- 60 days
- 90 days
- 180 days
- 365 days

Policy aggregate limit
- $250,000
- $500,000
- $1m
- $2m
- $3m
- $4m
- $5m
- $10m
- Other (please specify) _____

A. Risk questions

1. Estimated annual total number of transactions and records?
   Please combine the total of your client/customer records and total number of credit card transactions. For example, 5,000 customer records and 20,000 eftpos/credit transactions would give an 'annual total' of 25,000.
   - 0 – 10,000
   - 10,001 – 25,000
   - 25,001 – 50,000
   - 50,001 – 75,000
   - 75,001 – 100,000
   - 100,001 – 200,000
   - 200,001 – 300,000
   - 300,001 – 400,000
   - 400,001 – 500,000
   - 500,001 – 750,000
   - 750,001 – 1,000,000
   - 1,000,001 – 1,500,000
   - 1,500,001 – 2,000,000
   - 2,000,001 – 2,500,000
   - 2,500,001 – 5,000,000
   - 5,000,000 + (Please provide the total number) _____

2. Do you comply with your relevant Payment Card Industry Data Security Standard (PCI DSS) obligations?
   - Yes
   - No
   - Don't know
   - N/A – we are not subject to PCI DSS

3. What percentage of your Total Revenue is from online or e-commerce activities
   _____ %

4. Number of full time employees
   - 1 – 10
   - 11 – 20
   - 21 – 30
   - 31 – 50
   - 51 – 100
   - 101 – 200
   - 200+ (Please provide the number) _____

5. Do you have a Notifiable Data Breach plan in place and otherwise comply with The Privacy Act 2020 (Privacy Act)?
   - Yes
   - No
   - Don't know
   - N/A – we are not subject to the Privacy Act

6. Do you have a Data Protection/ Privacy policy?
   - Yes
   - No
   - Don't know

7. Do you have firewalls protecting your own and customer/client data?

- [ ] Yes
- [ ] No
- [ ] Don't know

8. Do you protect all all Personally Identifiable Information and other sensitive data through Encryption?

- [ ] Yes, info encrypted at rest on our network, in transit and when backed up
- [ ] Yes, info encrypted but ONLY in specific limited scenarios
- [ ] Yes, info encrypted in transit and when backed up but not when at rest on our network
- [ ] No, info not encrypted whatsoever

9. Do you outsource the handling of any Personally Identifiable Information?

- [ ] Yes
- [ ] No
- [ ] Don't know

10. Do you use up-to-date antivirus/ spyware and malware software?

- [ ] Yes, updated daily or automatically upon release
- [ ] Yes, updated on a weekly to monthly basis
- [ ] No
- [ ] Don't know

11. Are all mission/business critical systems and data information assets backed up and stored at another location?

- [ ] Yes, backed up daily
- [ ] Yes, backed up weekly or less frequently
- [ ] No
- [ ] Don't know

12. Has an independent party completed an audit of your system/data security?

- [ ] Yes
- [ ] No
- [ ] Don't know

13. If your IT network failed, which one of the following would best describe the impact to your operations and revenues?

- [ ] Inconvenience, very minimal revenue impact and operations could continue temporarily
- [ ] Revenues would NOT be impacted immediately, and only slightly when impacted
- [ ] Revenues would NOT be impacted immediately, but significantly when impacted
- [ ] Revenues would be impacted immediately but only slightly
- [ ] Revenues would be impacted immediately and significantly
- [ ] Operations and revenues would be entirely interrupted

14. Do you have written data security policies and procedures communicated to all employees, and do employees receive annual security awareness training?

- [ ] Yes, both written policies plus annual security awareness training
- [ ] Employee security awareness training but no written security policies
- [ ] Written policies but no employee security awareness training
- [ ] No
- [ ] Don't know

15. Are you aware of any claims, circumstances, privacy breaches, viruses, DoS/DDOS, or hacking incidents which have impacted, or could adversely impact your business?

- [ ] Yes
- [ ] No

If yes, please provide details including costs incurred and any remedial action taken

B. Please complete the following if your estimated revenue is over $25m or you have suffered a previous cyber loss.

1. Describe the type of information in records held by you
(Tick all that apply)

- ☐ Customer information (e.g. name, address, email address, phone etc.)
- ☐ Credit card details
- ☐ Personal identity information (e.g. drivers licence, TFN, passport number, government ID)
- ☐ Confidential third party trade secrets or IP (intellectual property)
- ☐ Banking or financial details
- ☐ Medical or healthcare data

2. Do you have a dedicated person responsible for your IT infrastructure, data security and privacy?

- ☐ Yes, full time IT Manager, Chief Information Security Officer (CISO) or similar
- ☐ Outsourced – IT contractor provides a full time dedicated person
- ☐ No, responsibility is shared amongst Legal, HR and other departments
- ☐ No
- ☐ Don't know

3. Do you have a Disaster Recovery Plan (DRP) and/or Business Continuity Plan (BCP) in place and has this been tested in the last 18 months?

- ☐ Yes, current and tested
- ☐ Yes, but not tested in the last 18 months
- ☐ Yes, but not ever tested
- ☐ No

4. Does your network include contingency / redundancy / resilience of any description, to mitigate system interruptions or failures (such as mirrored infrastructure, failover mechanisms, warm or hot replicated sites or similar)?

- ☐ Yes, multiple aspects
- ☐ Yes, but just one aspect
- ☐ No

5. Do you control / limit / monitor your employees' ability to remove data or information from your network / office (examples include USB drive security)?

- ☐ Yes, for data and physical information
- ☐ Yes, for data only
- ☐ Yes, for physical information only
- ☐ No

6. Does your website use web apps?
A web app is a software application which runs within a website rather than on your desktop. Web apps lend functionality and interactivity to websites. They let you do things on the site. Examples include interactive brochures, wikis, instant messaging, online sales, shopping carts, maps and many other functions.

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ N/A – we do not have a website

7. Do you use monitored Intrusion Detection or Intrusion Prevention Systems (IDS/IPS)?
Intrusion Detections and Intrusion Prevention Systems is software that monitors a network for unusual activity such as potential cyber threats and network traffic. Intrusion Prevention Systems have the additional capability of blocking intrusions and preventing hackers from exploiting vulnerabilities.

- ☐ Yes
- ☐ No
- ☐ Don't know

8. Are you aware of any evidence of network intrusion or vulnerabilities highlighted in an IT security audit or penetration test which have not yet been resolved?

- ☐ Yes
- ☐ No

If yes, please provide details

9. Have you had any unforeseen down time to your website or IT network of more than 12 hours?

- ☐ Yes
- ☐ No

If yes, please provide details

C. Please complete the following if your estimated revenue is over $75m or, you have suffered a previous cyber loss.

E-mail, RDP, O365

1. Do you authenticate inbound email? ☐ Yes ☐ No

If yes, indicate how ☐ DMARC ☐ DKIM ☐ SPF ☐ Don't know

2. Do you scan and filter inbound emails for malicious content (e.g. executable files)? ☐ Yes ☐ No ☐ Don't know

3. Does all remote access to your network and corporate email require multifactor authentication (MFA)? ☐ Yes ☐ No ☐ Don't know

4. Have you disabled remote desktop protocol (RDP)? ☐ Yes ☐ No ☐ Don't know

If no, have you implemented any of the following? ☐ VPN ☐ MFA ☐ RDP Honeypots ☐ No, none

5. Do you use O365 in your organisation? ☐ Yes ☐ No ☐ Don't know

If yes, indicate if any of the following have been implemented ☐ MFA ☐ ATP ☐ Macros disabled by default

If no, which product do you use for email monitoring (e.g. Proofpoint)?

6. Do you train end users against phishing and social engineering threats via ongoing campaigns and assessments? ☐ Yes, Annually ☐ Yes, Quarterly ☐ Yes, Monthly ☐ No ☐ Don't know

Backups

7. Do you take regular backups of critical data? ☐ Yes ☐ No ☐ Don't know

If yes, how frequently? ☐ Daily ☐ Weekly ☐ Monthly ☐ Other

8. Do you keep a copy of critical backups offline, segregated from and inaccessible to your network? ☐ Yes ☐ No ☐ Don't know

9. Where do you store backups? ☐ Cloud ☐ At a Secondary Data Centre ☐ Offline ☐ In a separate network segment

10. Which of the following have been implemented to secure the backup environment? ☐ Encryption ☐ Segmentation ☐ Vaulted Credentials ☐ MFA ☐ None of these

11. Do you use any commercial backup solutions (e.g. Commvault)?

☐ Yes ☐ No ☐ Don't know

If yes, which product(s) do you use?

☐ Don't know

12. Does your backup strategy include the use of immutable technologies?

☐ Yes ☐ No ☐ Don't know

13. Is the integrity of these backups and your recovery plans regularly tested?

☐ Yes ☐ No ☐ Don't know

Perimeter defence and privileges

14. Do you use an endpoint protection product (EPP)?

☐ Yes ☐ No ☐ Don't know

If yes, which product(s)?

☐ Don't know

15. Have you deployed an endpoint detection and response (EDR) tool that covers 100% of Servers and Endpoints?

☐ Yes - Servers ☐ No

☐ Yes - Endpoints ☐ Don't know

If yes, which product(s) do you use?

☐ Don't know

If the EDR tool offers AI/automated rules-based enforcement, has this been enabled?

☐ Yes ☐ No ☐ Don't know ☐ N/A

16. Do you operate a SIEM monitored 24/7/365 by an internal SOC or MSSP?

☐ Yes ☐ No ☐ Don't know

17. Do you enforce a BYOD (Bring Your Own Device) policy that ensures critical data is encrypted when transferred to portable media devices (USBs, laptops etc.)?

☐ Yes ☐ No ☐ Don't know

18. Do you allow local administrator rights on workstations?

☐ Yes ☐ No ☐ Don't know

19. Do administrative/privileged accounts utilise a privilege access management (PAM) tool (e.g. CyberArk)?

☐ Yes ☐ No ☐ Don't know

If yes, which product do you use?

☐ Don't know

Incident response plan

20. Does your incident response plan (IRP) specifically address ransomware scenarios?

☐ Yes ☐ No ☐ Don't know ☐ We don't have an IRP

If you answered 'No' to any of the above, please detail below along with mitigating comments

Please outline any additional controls your organisation has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, use of unique credentials, vulnerability scanning, etc.)

D. Optional covers

1. Optional cover – Contingent Business Interruption

a. Do you want optional cover for Contingent Business Interruption?
If an external supplier suffers a cyber event that causes Business Interruption to the insured business, Ando Data Insurance covers the impact on the insured's business costs.

☐ Yes ☐ No

b. 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

2. Optional cover – Criminal Financial Loss

a. Do you want optional cover for Criminal Financial Loss?
Includes Cyber Theft, Telephone Phreaking, Identity-based Theft and Cryptojacking. Does not include Socially Engineered Theft unless selected below.

☐ Yes ☐ No

b. Aggregate limit for Criminal Financial Loss

☐ $10,000 ☐ $25,000 ☐ $50,000 ☐ $75,000
☐ $100,000 ☐ $150,000 ☐ $250,000 ☐ Other (please specify) _____

c. Do you want to include cover for Socially Engineered Theft?

☐ Yes ☐ No

d. Sublimit for Socially Engineered Theft
The sublimit for Socially Engineered Theft cannot be greater than the aggregate limit for Criminal Financial Loss.

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

e. Do you require passwords to be changed regularly? (at least quarterly)

☐ Yes ☐ No ☐ Don't know

f. Do you allow remote access to your internal network?

☐ Yes ☐ Yes, with dual authentication
☐ No ☐ Don't know

g. Are all new payees, and changes to existing payees' banking details, double authenticated with the payee?

☐ Yes ☐ No ☐ Don't know

h. Do transfers greater than $10,000 require dual signature or supervisor/manager sign off?

☐ Yes ☐ No ☐ Don't know

i. Are you entrusted with or in control of funds from a 3rd party, or do you provide any of the following services for others? (tick all that apply)

☐ Collection or payment processing
☐ Asset, investment or trust management services
☐ Cash management or other treasury functions
☐ Other office functions

If 'Other office functions' is selected, please provide details

j. Have you ever been declined for Crime, Fidelity or Computer Crime insurance, or had such insurance cancelled?

☐ Yes ☐ No ☐ N/A, have never had such insurance

If 'yes' please provide details

k. Have you ever suffered a Crime, Fidelity or Computer Crime loss?

☐ Yes ☐ No ☐ N/A

If 'yes' please provide details

3. Optional cover – Tangible Property

a. Do you want optional cover for Tangible Property?

☐ Yes ☐ No

b. Aggregate limit for Tangible Property

☐ $5,000 ☐ $10,000 ☐ $15,000
☐ $25,000 ☐ $50,000 ☐ Other (please specify) _____

4. Optional cover – Joint Venture and Consortium cover

a. 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 joint venture or consortium for the coming 12 months in your estimated total revenue.

The Insurer

The insurer is Ando Insurance Group Limited as agent of Emergence Insurance Pty Ltd on behalf of certain underwriters at Lloyd's (the Underwriters).

Declaration

Privacy authorisation

You agree to Ando Insurance Group Limited collecting, using and disclosing your personal information as set out in our Privacy Policy. Where you provide us with personal information about any other person for insurance related purposes, you confirm that you have the authority of those persons to disclose such information and to authorise Ando to collect, hold, use and disclose the information in accordance with our Privacy Policy. For information about Ando's Privacy Policy, please see ando.co.nz/privacy-policy

Duty of Disclosure

You must tell us all information you know (or could reasonably be expected to know) which would influence our decision, and the judgement of a prudent Underwriter, whether or not to accept your proposal, and if it is accepted, on what terms including the excess and at what cost. You also have this duty to disclose all material information on each renewal of insurance cover and when you make changes to it.

Examples of information you may need to disclose include:

- any insurance claim you have made in the past;
- anything or any known circumstances that might increase the risk of an insurance claim;
- if another insurer has cancelled or refused to renew insurance, or has imposed special terms;
- previous criminal convictions, or pending criminal charges^;
- any previous bankruptcy or having been through the 'No Asset Procedure'.

Examples of information you do not need to disclose include:

- anything that is common knowledge;
- anything that reduces the risk of an insurance claim;
- anything we say you do not need to tell us about;
- anything you have already told us, or that we should be expected to know in the ordinary course of our business.

These examples are a guide only. You are under this duty to disclose all material information whether the information is asked for or not. All information given must be complete and correct. If you have any doubt as to whether a fact is material, then it should be disclosed.

^ Subject to the rights set out in the Criminal Records (Clean Slate) Act 2004 ("Clean Slate Act").

I/we:

- declare that the information provided in this proposal and any other supplied information is in every way correct and complete and all material information has been disclosed.
- agree that the information provided in this proposal and any other supplied information will form the basis of any insurance contract that may be offered and that I/we will accept cover on the terms and premium prescribed by Ando.
- authorise Ando to give to and obtain from other insurance companies, insurance brokers, the Insurance Claims Register Ltd or any other party information about this insurance, any insurance held by me/us and any claims made by me/us.
- authorise Ando to use the information provided to advise me/us of their other products and services.

By signing this declaration you are confirming to us that you have disclosed all information relevant to acceptance of the proposal and in accordance with your duty of disclosure.

☐ I have read and accept these conditions (please tick)

Name _____ Date _____

Signature _____

For more information, contact your broker or visit us online **ando.co.nz**

ORG08025/V001