DUAL Cyber Insurance

Proposal form

Revenues between $100m and $1bn

IMPORTANT NOTICES

Please read the following before proceeding to complete this proposal form.

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, that 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:

a. reduces the risk we insure you for;

b. is common knowledge;

c. we know or should know as an insurance company; or

d. we waive your duty to tell us about.

If you do not tell us something

If you do not tell us something you are required to, we may cancel your policy or reduce the amount we shall indemnify 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.

Completing this Proposal Form

- Please answer all questions giving full and complete answers.
- It is the duty of the Applicant to provide all information that is requested in the Proposal Form as well as to add additional relevant fact.
- Note: a relevant fact is such known fact and/or circumstance that may influence in the evaluation of the risk by the Insurer. If you have any doubts about what a relevant fact is, please do not hesitate to contact your broker.
- If the space provided on the Proposal Form is insufficient, please use a separate signed and dated sheet in order to provide a complete answer to any question.
- The Proposal Form must be completed, signed and dated by a person who must be of legal capacity and authorised for the purpose of requesting management liability insurance for the organisation who acts as the Applicant.

This Proposal Form DOES NOT BIND the Applicant or the Insurer to complete the insurance but will form part of any insurance.

Privacy Collection Statement

At DUAL New Zealand, we are committed to protecting your privacy and complying with the Privacy Act 2020 (NZ) (Privacy Act).

We use your information to assess the risk of providing you with insurance, provide quotations, issue policies and assess claims, on behalf of the insurers we represent. We also use your information to administer any policies we have issued to you and may do so by mail or electronically unless you tell us that you do not wish to receive electronic communications. If you do not provide us with full information, we may not be able to provide insurance or assess a claim. If you provide us with information about someone else, you must obtain their consent to do so.

We provide your personal information to the insurers we represent when we issue and administer your insurance. When providing a quotation or insurance terms, we will tell you if the insurers is overseas and if so, where they are. We may also provide your information to your broker and our contracted third-party service providers (e.g.,claims management companies and AI cyber risk quantification platforms). We are part of Howden Group Holdings Limited and may provide your information to UK based Group entities who provide us with business support services. If a recipient is not regulated by laws which protect your information in a way that is similar to the Privacy Act, we will take reasonable steps to ensure that they protect your information in the same way we do or seek your consent before disclosing your information to them. We do not trade, rent or sell your information.

Our Privacy Policy contains more information about how to access and correct the information we hold about you and how to make a privacy related complaint, including how we will deal with it. By providing us with your personal information, you consent to its collection and use as outlined above and in our Privacy Policy.

Ask us for a copy of our Privacy Policy via email at privacy@dualnewzealand.co.nz or access it via our website using the following link.

Section 1 - Details of the applicant

1. Insured Entity Type (please select):

- ☐ Sole Trader
- ☐ Unlisted Limited Company
- ☐ Partnership
- ☐ Not for profit / Association
- ☐ Public Listed Company
- ☐ Private Company (Pty Ltd)

2. ABN/ACN:

3. Insured Name:

4. Trading Name (if applicable):

5. Insured's Registered Address:
(Place where business is registered/place of incorporation.)

6. Date Established:

7. Insured's Website Address:

- ☐ N/A - Insured does not have a website

8. Number of employees:

9. Occupation/Business Description:
Please provide a detailed description of all business activities including the activities of any related entities.

Section 2 - Business and employee information

Subsidiaries

1. Are you domiciled in New Zealand with no subsidiaries outside New Zealand or Australia? Yes ☐ No ☐

   If NO, please confirm:

   a. Are you domiciled in New Zealand? Yes ☐ No ☐

   b. Where are the Insured's overseas subsidiaries?

Please specify below in which countries the Insured's subsidiaries are located and indicate the percentage of total revenue derived.

Subsidiary Name	Country	Revenue %

Turnover

2. Please provide:

	Past Year	Current Year	Estimated Next Year
Total Turnover (NZD)			
% of Turnover Derived from Online Channels			
% of Approximate Gross Profit			

3. Is more than 25% of the Insured's revenue derived from the USA and Canada? Yes ☐ No ☐

4. Is the policyholder a subsidiary, franchisee or smaller company of a larger group? Yes ☐ No ☐

   If YES, please provide details about any network interconnectivity and/or segmentation with those organisations:

5. Is the Insured exempt from GST? Yes ☐ No ☐

Section 3 - Identity and Access Management

1. Is multi-factor authentication required for any and all remote access to the following systems/services/platforms:

   a. Remote access to your network? Yes ☐ No ☐ N/A ☐

   b. Web-based or cloud hosted email? Yes ☐ No ☐ N/A ☐

   c. Critical cloud resources or cloud resources holding sensitive information? Yes ☐ No ☐ N/A ☐

   If NO, please provide details on other mitigating controls required for remote access:

Section 4 - Email Security

1. Do you have an e-mail filtering system in place (such as Mimecast or Proofpoint, or system native tools such as Microsoft's Exchange Online Protection (EOP) or Defender) that is activated for all email accounts? Yes ☐ No ☐

2. Do you authenticate outbound emails through:

   a. Domain Keys Identified Mail (DKIM) Yes ☐ No ☐

   b. Domain-based Message Authentication, Reporting and Conformance (DMARC) Yes ☐ No ☐

   c. Sender Policy Framework (SPF) Yes ☐ No ☐

Section 5 - Privileged Access Management

1. Please indicate which of the following measures are in place for the protection of privileged credentials

   ☐ Privileged user accounts have separate/unique credentials from their everyday accounts

   ☐ Privileged Accounts are controlled by a Privileged Access Management (PAM) solution

   ☐ Multi-Factor Authentication is required for all administrator/privileged accounts

   ☐ Access logs are retained for at least 90 days

2. How many does the policy holder have of the following:

   a. Global admin accounts:

b. Domain or other on premises admin accounts:

c. Privileged service accounts:

Section 6 - Business Continuity, Disaster Recovery & Resilience

1. Please select all that apply in respect of your back up environment:

- ☐ Immutable or Write Once Read Many (WORM) technologies used
- ☐ Cloud hosted back ups
- ☐ Access to backups via Multifactor Authentication
- ☐ Offline/Air-gapped back ups disconnected from the rest of the network
- ☐ Encrypted
- ☐ Restricted access via separate privileged accounts

2. How often do you validate system restoration capabilities by performing a full restore using a sample set of back up data?

☐ Quarterly or more regularly ☐ Biannually ☐ Annually

☐ Other **(please provide further information here)**

3. Please confirm which of the following formal plans you have in place (which address 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 ☐
Cyber Incident Response Plan	Yes ☐ No ☐	Yes ☐ No ☐

4. Does your organization implement structured and documented network segmentation to clearly separate environments and restrict unauthorised lateral movement (e.g. segmenting retail/branch networks, business units, and critical systems)?

- ☐ Yes (segmented with enforced controls and regular validation)
- ☐ Partial (limited segmentation)
- ☐ No

Section 7 - End of Life Technology

1. Do you use any end-of-life or unsupported operating systems or software including on an extended support basis? Yes ☐ No ☐

   If YES, please answer the following questions:

   a. Is the system segregated from other environments (e.g. through air-gapping, VLAN segmentation, or firewall controls)? Yes ☐ No ☐

   b. Is any of this hardware, software, or systems business critical? Yes ☐ No ☐

2. Please describe any additional security controls implemented to mitigate the risk of vulnerability exploitation:
   (E.g Plans to decommission, restricted from internet access)

Section 8 - Data Management & Privacy

1. Approximately how many unique individuals and organisations would you be required to notify in the event of a breach of Personally Identifiable Information (PII)?

2. Please indicate the types of PII your organisation holds:

   ☐ Basic customer information (e.g. name, address, email address, phone number)

   ☐ Payment card information

   ☐ Personal identity information (e.g. driver's licence, tax file number, passport number)

   ☐ Banking or financial information

   ☐ Medical or healthcare data

3. Is all sensitive, confidential, critical or valuable data encrypted? Yes ☐ No ☐

   If YES, which of the following:

   ☐ At rest on the network ☐ In transit ☐ In back-up

4. Does your organisation have a company wide policy that ensures compliance with applicable privacy and data protection laws and regulations relevant to your industry and the jurisdictions in which you operate? Yes ☐ No ☐

If NO, please describe how you address privacy and data protection laws within your organisation:

5. Does your organization have a formal policy for disposing of or purging PII that is no longer required to be retained? Yes ☐ No ☐

If NO, please explain how your organisation ensures that PII no longer required is properly and securely disposed of:

Section 9 - Endpoint / Asset Security

1. Do you utilize an endpoint detection and response (EDR) solution across your network environment? Yes ☐ No ☐

If YES, which product do you use:

2. What percentage of endpoints are covered?

☐ 0-20% ☐ 21-50% ☐ 51-75% ☐ 76-99%

3. Are alerts from your endpoint detection solution integrated into a Security Information and Event Management (SIEM) or similar system? Yes ☐ No ☐ Partial ☐

4. Does your organisation operate a Security Operations Centre (SOC) to monitor and manage security events?

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

If YES, is it internally or externally managed?

☐ Internal ☐ External ☐ Both

Section 10 - Patch Management

1. Please describe your patch management process, including how you ensure that all critical patches are applied promptly. Additionally, specify the typical timeframe for deploying patches addressing zero day vulnerabilities once the vendor releases them:

2. Are patches tested in a UAT environment before being deployed in the live environment? Yes ☐ No ☐

Section 11 - Social Engineering and Cyber Fraud

1. Do you wish to have cover for Social Engineering and Cyber Fraud? Yes ☐ No ☐
(Please note there may be an additional premium)

   For further information regarding this Optional Extension, please visit our website.

   If YES please confirm the following, or if NO please continue to Section 12.

   a. When creating or amending supplier and customer payment details, does the Insured independently verify the details with a known contact by phone or in person? Yes ☐ No ☐

   b. Does the Insured ensure that at least two members of staff authorise any transfer of funds, signing of cheques (above $10,000) and the issuance of instructions for the disbursement of assets, funds or investments? Yes ☐ No ☐

   c. Does the Insured maintain procedures for the provision of written training materials to all Employees regarding the dangers of Social Engineering Fraud, Phishing, and Cyber Fraud which incorporate regular review? Yes ☐ No ☐

   d. Does the Insured implement procedures for accessing any and all online financial accounts and banking platforms requiring either: Yes ☐ No ☐

      i. two factor authentication; or

      ii. the requirement that passwords are changed at least every 45 days; or

      iii. the implementation of long passwords of 12 characters or more requiring at least 3 special characters?

2. Do you employ a third party payment verification platform to validate supplier banking details and mitigate payment redirection fraud (e.g. Eftsure)? Yes ☐ No ☐

   If YES, please provide the name of the product used:

Section 12 - Non-IT Contingent Business Interruption

1. Do you wish to have cover for non-IT Contingent Business Interruption? Yes ☐ No ☐
   (Please note there may be an additional premium)

   If YES, please answer the following questions:

   a. Are all critical components, services and supplies readily available from multiple sources? Yes ☐ No ☐

   b. Are critical components, services and supplies available within 10 days from new sources? Yes ☐ No ☐

   c. Does it take longer than 10 days for substitutes to become available, or is substitution not possible? Yes ☐ No ☐

2. Does the organisation conduct formal due diligence, including IT and cybersecurity due diligence, on all third party suppliers as part of its supplier risk management process? Yes ☐ No ☐ Partial ☐

Section 13 - Regulatory issues

1. Have you ever been investigated in respect of personally identifiable information, including but not limited to payment card information, or your privacy practices? Yes ☐ No ☐

2. Have you been asked to supply any regulator or similar body with information relating to personally identifiable information or your privacy practices? Yes ☐ No ☐

3. Have you ever been asked to sign a consent order or equivalent in respect of personally identifiable information or your privacy practices? Yes ☐ No ☐

4. Have you ever received a complaint relating to the handling of someone's personally identifiable information? Yes ☐ No ☐

   If YES, please specify details (attach additional information if required):

Section 14 - Claim details

1. After enquiry of all Partners, Principals, Directors, Officers, Trustees and Senior Managers:

   a. Have there been any claim(s) made against the Insured or any loss or expense incurred* which might fall within the terms of this insurance cover?

OR

Yes ☐ No ☐

b. Have any circumstances occurred which may give rise to a claim against the Insured or result in any loss or expense incurred* which might fall within the terms of this insurance cover?

***Incurred means any settlement made, legal fees, defence costs or reserved amounts.**

If YES, please provide further information (attach additional information if required):

2. Is the Insured aware of any matter that is reasonably likely to give rise to any loss or claim under such insurance, or has the Insured suffered any loss or any claim including but not limited to a regulatory, governmental or administrative action brought against the Insured, or any investigation or information request concerning any handling of personally identifiable information?

Yes ☐ No ☐

If YES, please provide further information (attach additional information if required):

3. Has the Insured or any Partners, Principals, Directors, Officers, Trustees and Senior Managers ever been declined this type of insurance, or had similar insurance cancelled, or had an application for renewal declined (other than insurer exiting that area of insurance), or had special terms or restrictions imposed?

Yes ☐ No ☐

Section 15 - Indemnity limit

1. Does the Insured currently have Cyber Liability and Data Protection insurance in place?

Yes ☐ No ☐

If YES, please provide details:

Name of Insurer:	
Limit of Indemnity:	
Deductible:	
Expiry Date of Policy:	
Retroactive Date of the Policy:	

2. Please select the amount of Indemnity required:

☐ NZD 500,000 ☐ NZD 1,000,000 ☐ NZD 2,000,000

☐ NZD 3,000,000 ☐ NZD 4,000,000 ☐ NZD 5,000,000

☐ NZD 10,000,000 ☐ Other (please state):

3. Does the Insured wish to change their limit structure from an aggregate limit to an any one claim limit? Yes ☐ No ☐

Eligibility for this cover is limited to clients with annual revenue of less than $250,000,000 and an additional premium may apply.

Section 16 - Operational Technology

1. Does the policyholder use operational technology? Yes ☐ No ☐

If YES, please answer the following questions:

Operational Technology (OT) refers to hardware and software systems that monitor and control industrial processes, such as manufacturing, energy, utilities, and transportation.

a. Is Operational Technology segregated from main IT environment? Yes ☐ No ☐

b. Can Operational Technology be accessed remotely? Yes ☐ No ☐

If YES, is MFA enforced? Yes ☐ No ☐

2. Are manual alternatives or redundancies in place for Operational Technology downtime Yes ☐ No ☐

Declaration

Signing this Proposal Form does not bind the proposer or the Insurer to complete this insurance

The undersigned declares that the statement and particulars in this Proposal Form are true and that no material facts have been misstated or suppressed after enquiry. The undersigned agree that should any of the information given by us alter between the date of this proposal and the inception date of the insurance to which this proposal relates, the undersigned will give immediate notice thereof. The undersigned agrees that the Underwriters may use and disclose our personal information in accordance with the 'Privacy Collection Statement' at the beginning of this proposal.

The undersigned acknowledges that they have read the policy wording and associated endorsements and are satisfied with the coverage provided, including the limitations and restrictions on coverage.

The undersigned also acknowledges that the insurance is being purchased for business purposes only, and not wholly or predominately for personal, domestic or household purposes. This product therefore does not constitute a consumer insurance contract pursuant to the Financial Markets Conduct Act 2013. If the insurance is being considered for personal, domestic or household purposes, please contact your broker for further information.

The undersigned agrees that this proposal, together with any other information supplied by us shall form the basis of any contract of insurance effected thereon.

To be signed by the Insured for whom this insurance is intended for

Full name:

Position:

Signature:

Date:

It is important the undersigned of the declaration above is fully aware of the scope of this insurance so that these questions can be answered correctly. If in doubt, please contact the broker or agent, since non-disclosure may affect an Insured's right of recovery under the policy.

DUAL New Zealand recommends that you keep a record of all information supplied for the purpose of entering into an insurance contract (including copies of this Proposal Form and correspondence).

IMPORTANT NOTICES

Claims Made and Notified and Covered Events Discovered Policy

This is partly a claims made and notified policy and partly a discovery policy. We shall only cover you for:

- claims made against you during the insurance period and notified to us as soon as practicable during the insurance period; or
- covered events first discovered and notified to us as soon as practicable during the insurance period.

If your policy does not have a continuity of cover provision or provide retrospective cover then your policy may not provide insurance cover in relation to events that occurred before the policy was entered into.

Notification of Claims

In the event of a claim arising under this Insurance, immediate notice should be given to:

Atmos

Telephone: +64 800 656 155

or at dualresponse@atmosgroup.co.nz

Please refer to the Claims Conditions section of this policy for further details regarding the notification of claims or loss subject to this Insurance.

Contract by the Insured Affecting Rights of Subrogation

If the proposed contract of insurance includes a provision which excludes or limits the Insurer's liability in respect of any loss because you are a party to an agreement which excludes or limits your rights to recover damages from a third party in respect of that loss, you are hereby notified that signing any such agreement may place your indemnity under the proposed contract of insurance at risk.

Surrender or Waiver of any Right of Contribution or Indemnity

Where another person or company would be liable to compensate you or hold you harmless for part or all or any loss or damage otherwise covered by the Policy, but you have agreed with that person either before or after the inception of the Policy that you would not seek to recover any loss or damage from that person, you are NOT covered under the Policy for any such loss or damage.