Cyber proposal form

Security & privacy protection

Important notices to applicants regarding the completion of this proposal form

Duty to make a fair presentation of the risk/ disclose material information

From 12 August 2016, the duty of disclosure for commercial insurance contracts changed with the implementation of the Insurance Act 2015 ("The Act"). For risks incepting or renewing on or after 12 August 2016, you have a duty to make "a fair presentation of the risk". To meet this duty, you need to disclose all material information to Insurers which is known to you (or which ought to be known to you). Information is material if it would influence the judgement of a prudent insurer in establishing the premium or determining whether to underwrite the risk and, if so, on what terms. Material information does not necessarily have to actually increase the risk of the insurance under consideration.

Data Protection Act 1998

The information, which you provide to us, along with other related information, will be held by DUAL Corporate Risks Limited and used to administer your insurance requirements. All enquiries about our data protection policy should be addressed to: Head of Compliance, DUAL Corporate Risks Limited.

01. General information

Name & address of applicant

Full name .....

Company name .....

Street ..... City .....

Postcode ..... Country .....

Website .....

Business activities

01. General information continued

Annual revenue (GBP)

	Last complete financial year	Current year (estimate)	Next year (estimate)
UK revenue			
US revenue			
ROW revenue*			

*For ROW revenue, please provide a split of revenue by country as an appendix to this application

02. Risk assessment

Data

1 Please estimate the total number of unique individuals for whom records are currently stored by the applicant

Network security assessment

		Yes	No
1	Does the applicant Conduct Vulnerabilty assessments / penetration tests of its network at least annually?	☐	☐
	If so, please can you confirm that critical deficiencies are remediated	☐	☐
2	Have firewalls at all external connection points?	☐	☐
3	Run anti-virus on its network?	☐	☐
4	Operate a patch management strategy?	☐	☐
5	Have intrusion prevention or detection software in place?	☐	☐
	If yes, is there a process in place to review intrusion logs and immediately escalate critical alerts?	☐	☐
6	Permit remote access to its corporate network?	☐	☐
	If yes, is this limited to two-factor authentication only?	☐	☐

Handling sensitive or critical data

Does the applicant:		Yes	No
1	Isolate critical/sensitive information in its own segregated environment?	☐	☐
2	Encrypt critical/sensitive information whilst at rest?	☐	☐
3	Encrypt critical/sensitive information in transit?	☐	☐

02. Risk assessment (continued)

Mobile & portable devices

Does the applicant:	Yes	No
1 Store sensitive data on any mobile or portable device, including back-up tapes?	☐	☐
If yes, is such sensitive data encrypted?	☐	☐
2 Permit Bring-Your-Own-Device (BYOD)?	☐	☐
If yes, does the applicant have a policy that governs BYOD usage and controls?	☐	☐

Data recovery & network business interruption assessment

Does the applicant:	Yes	No
1 Back-up all sensitive/critical data at least daily?	☐	☐
If yes, are these back-ups stored off-site?	☐	☐

2 How long does it take to restore the applicant's critical systems following a network outage?

☐ Less than 8 hours ☐ Between 8 and 12 hours

☐ Between 12 and 24 hours ☐ More than 24 hours

Incident management

1 Please tick below to indicate which of the following the applicant has in place?

☐ Business Continuity Planning

☐ Incident response plan

☐ Disaster recovery plan

	Yes	No
2 Does the applicant test these plans at least annually?	☐	☐

Multimedia assessment

Does the applicant:	Yes	No
1 Have a process in place to review media content (website, social media or otherwise prior to publication)?	☐	☐
2 Have processes in place to take down content that is deemed offensive?	☐	☐

02. Risk assessment (continued)

Claims & insurance history

		Yes	No
1	In the last 5 years, has the applicant received or sustained, or is there currently pending, any claims, complaints or incidents which may be covered under the proposed insurance and/or does the applicant have knowledge of any fact, circumstance, situation, event or transaction which may give rise to a claim or loss under the proposed insurance?	☐	☐

Insurance history

		Yes	No
1	During the last 5 years, has any insurance policy providing materially the same or similar insurance as the insurance being applied for under this application been declined, cancelled or non-renewed at the decision of the insurer?	☐	☐
2	Does the applicant presently procure a stand-alone cyber insurance policy?	☐	☐

If you entered no for any of the above please provide further details.

Declaration

I/We declare that the answers to the questions in this proposal form are true and accurate having consulted with all partners or directors and other persons involved in the management of the applicant firm.

This application must be signed by a corporate officer with authority to sign on the applicant's behalf.

I/we understand that the information provided will be used in deciding whether the insurer will accept the application, the terms of any policy provided and the price charged by the insurer for the risk

Signed ..... Title .....

Print name ..... Date .....

03. Supplementary questions

Payment card industry assessment

Does the applicant: | **Yes** | **No**

1 Accept credit card payments for its good or services? ☐ ☐

If yes: | **1.** | **2.** | **3.** | **4.**

i) What level of PCI merchant is the applicant? ☐ ☐ ☐ ☐

ii) What is the approximate percentage of annual revenue attributable to credit card transactions? .....

iii) How many credit or debit card transactions does the applicant process annually? .....

2 Is the applicant compliant with Payment Card Industry Data Security Standards as of this application date? ☐ ☐

3 Does the applicant store credit card data on its network? ☐ ☐

If yes:

i) Is credit card data either encrypted or tokenised at all times? ☐ ☐

ii) If the credit card data is not encrypted or tokenised, how is it secured?

4 Is credit card data sent to a payment processor? ☐ ☐

If yes, has the payment processor provided evidence of its PCI compliance to the applicant? ☐ ☐

03. Supplementary questions (continued)

Vendor management

1 Please identify all vendors that have access to the applicant's data or who help to manage the applicant's network or security systems

Name of vendor	Nature of service

	Yes	No
1 Are vendor access rights periodically reviewed?	☐	☐
2 Is vendor access on the applicant's network monitored?	☐	☐
Does the applicant comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which it operates? (eg Data Protection Act, EU Data Protection Regulations, Australian Data Privacy Principles)	☐	☐