DUAL Cyber

Security and privacy protection

Proposal form

Security and privacy protection proposal form

Important notice concerning disclosure of material information

We take this opportunity to remind you that you owe a duty to make a fair presentation of the risk to the insurer. You have a duty to disclose to the insurer every material circumstance which you know or ought to know after a reasonable search or which is sufficient to put the insurer on notice that it needs to make further enquiries for the purpose of revealing those material circumstances. In addition, you have a duty to disclose information in a clear and accessible manner.

A circumstance is material if it would influence a prudent insurers judgment in determining whether to take the risk and, if so, on what terms. Failure to disclose a material circumstance may entitle an insurer to:

- in some circumstances, avoid the policy from inception and in this event any claims under the policy would not be paid;
- impose different terms on your cover; and/or
- reduce the amount of any claim payable.

This duty applies:

- before your cover is placed;
- when it is renewed; and
- at any time that it is varied.

General Data Protection Regulation

Any information about **You** which you provide to **Us** will be processed by **Us** in compliance with the General Data Protection Regulation, for the purpose of providing insurance and handling claims, if any, which may necessitate providing such information to third parties.

General information

01. Name and address of applicant:

Company name:

Street:

City:

Postcode:

Country:

Website:

Staff number:

Business activities

01. Please describe:

Turnover/Income

Year end:

Currency:

	Last complete financial year	Current year (estimate)	Next year (estimate)
UK turnover/income:			
US turnover/income:			
Rest of World (ROW)* turnover/income:			

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

Risk assessment

Data

01. Please advise approximate number of Personally Identifiable Information (PII*) Records stored on your network, database or system:

*PII is defined as a personally identifiable record that can be used to identify, contact or locate a single individual.

02. Does the applicant:

a) Isolate critical/sensitive data in its own segregated environment? Yes ☐ No ☐

b) Encrypt critical/sensitive data whilst 'at rest'? Yes ☐ No ☐

c) Encrypt critical/sensitive data 'in transit'? Yes ☐ No ☐

Network security assessment

Do you:

01. Conduct penetration tests of your network at least annually? Yes ☐ No ☐

If **yes**, please confirm that all high critical findings / recommendations have been remediated /actioned: Yes ☐ No ☐

02. Have firewalls at all external connection points? Yes ☐ No ☐

03. Run anti-virus on your network? Yes ☐ No ☐

04. Have intrusion prevention or detection software in place? Yes ☐ No ☐

If **yes**, is there a process in place to review intrusion logs and immediately escalate critical alerts? Yes ☐ No ☐

Mobile and portable devices

Does the applicant:

01. Store sensitive data on any mobile or portable device, including back-up tapes? Yes ☐ No ☐

If **yes**, is such sensitive data encrypted? Yes ☐ No ☐

02. Permit Bring-Your-Own-Device (BYOD)? Yes ☐ No ☐

If **yes**, does the applicant have a policy that governs BYOD usage and controls? Yes ☐ No ☐

Data recovery and network business interruption assessment

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

☐ Less than 8 hours ☐ Between 12 and 24 hours

☐ Between 8 and 12 hours ☐ More than 24 hours

Network security

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

☐ Business continuity planning ☐ Incident response plan

☐ Disaster recovery plan

02. Are these regularly tested and updated (at least annually)? Yes ☐ No ☐

If **no**, when was the last test/update conducted?

Multimedia assessment

Does the applicant:

01. Have a process in place to review media content (website, social media or otherwise prior to publication)? Yes ☐ No ☐

02. Have processes in place to take down content that is deemed offensive? Yes ☐ No ☐

Vendor management

01. 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

02. Do vendors have access rights to the applicant's network? Yes ☐ No ☐

i) If **yes**, are vendor access rights periodically reviewed? Yes ☐ No ☐

ii) Is vendor access on the applicant's network monitored? Yes ☐ No ☐

03. Does the applicant comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which it operates? (E.g. Data Protection Act, EU Data Protection Regulations, Australian Data Privacy Principles.) Yes ☐ No ☐

Payment card industry assessment

01. Does the applicant accept credit card payments for its good or services? Yes ☐ No ☐

If **yes**:

i) What level of PCI merchant is the applicant? 1 ☐ 2 ☐ 3 ☐ 4 ☐

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?

02. Is the applicant compliant with Payment Card Industry Data Security Standards as of this application date? Yes ☐ No ☐

03. Does the applicant store credit card data on its network? Yes ☐ No ☐

If **yes**:

i) Is credit card data either encrypted or tokenised at all times? Yes ☐ No ☐

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

04. Is credit card data sent to a payment processor? Yes ☐ No ☐

If **yes**, has the payment processor provided evidence of its PCI compliance to the applicant? Yes ☐ No ☐

Claims and event history

During the past 12 months, has the company:

01. Experienced any unscheduled or unintentional network outage, intrusion, corruption or loss of data? Yes ☐ No ☐

02. Become aware of any privacy violations or compromise of Personally Identifiable Information? Yes ☐ No ☐

03. Notified any customers that their information may have been compromised? Yes ☐ No ☐

04. Become aware of any circumstance or incident that could be reasonably expected to give rise to a claim against the cyber insurance policy under consideration? Yes ☐ No ☐

05. In the last five 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? Yes ☐ No ☐

If **yes** to any of the above, please provide details:

Insurance history

01. Does the applicant presently procure a stand-alone cyber insurance policy? Yes ☐ No ☐

02. During the last five 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? Yes ☐ No ☐

If you entered **yes** to the above, please provide further details:

Ransomware

01. Please confirm that an email filtering system is used and that the system is activated for all email accounts? Yes ☐ No ☐

02. Does the email filter provide the following protections? Please tick all that apply:

☐ Screenings for malicious attachments/links ☐ Quarantine service

☐ Reputation checks ☐ Email fraud defence (DMARC)

03. Do you use Office 365 in your organisation? Yes ☐ No ☐

If **yes**, tick all that apply:

☐ Office 365 Advanced Threat Protection add-on ☐ Multi-factor authentication for all users of Office 365

04.	Do you use endpoint detection and response (EDR) tools for malware protection?	Yes ☐	No ☐
05.	Do you have a Security Operations Centre (SOC) in place?	Yes ☐	No ☐
	If **yes**, tick all that apply:	24/7 ☐ MSSP ☐	SIEM ☐
06.	Please confirm you secure any and ALL remote access to their corporate network or any cloud-based services by requiring multi-factor authentication. This relates to access by any party, including third party vendors granted authorised access, via any means other than a wired connection to the company network when at a physical location owned or operated by the insured.	Yes ☐	No ☐
07.	Do you use multi-factor authentication to protect privileged user accounts?	Yes ☐	No ☐
08.	Are access controls based upon the principle of least privilege?	Yes ☐	No ☐
09.	Do you back up critical data regularly (minimum once per week)?	Yes ☐	No ☐
10.	Are your back-ups disconnected from and inaccessible through the organisation's network and/or do you use a dedicated cloud storage provider, designed for this purpose?	Yes ☐	No ☐
11.	Do you test the successful restoration and recovery of key server configurations and data from back-ups?	Yes ☐	No ☐
12.	Do you have a secure/hardened baseline configuration which is regularly reviewed and updated by someone with the security expertise and/or in line with industry standards?	Yes ☐	No ☐
13.	Have you undertaken a network scan regarding unauthorised access/malware etc. within the past 60 days?	Yes ☐	No ☐
14.	Confirmation that processes are in place to identify and apply patches within 30 days of release:	Yes ☐	No ☐

15. If you answered **no** to any of the above, please provide additional details:

16. Please describe any additional steps your organisation takes to detect and prevent ransomware attacks (network segmentation, software tools, external security services, penetration tests, vulnerability testing etc.):

Declaration

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.

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

Title:

Name of partner/director:

Signature of partner/director:

Date:

DD MM YYYY

A copy of this proposal should be retained by you for your own records.

Helping you do more

One Creechurch Place, London EC3A 5AF

+44 (0)20 7337 9888
enquiries@dualgroup.com
dualinsurance.com