HISCOX

Cyber and data
Proposal form

1. Your business

Business name

Main address

Postcode

Year business established:

Website:

1.1 Your employees

Your total number of employees (including subsidiaries)

1.2 Subsidiary or associated companies

Do you require cover for any subsidiary or associated companies? Yes ☐ No ☐

If **yes**, you must ensure that all other information you give in this proposal form incorporates that for the subsidiary or associated companies, including income and claims information.

You must also provide a separate list of subsidiary and associated companies.

1.3 Accredited information security standards

Has your organisation been accredited with any information security standards? Yes ☐ No ☐

If **yes**, please provide details:

1.4 Business activities

Please describe the nature of your business activities and include those of any subsidiaries that you want to be covered:

1.5 Your financial details

Please provide your turnover including fee income:

	Past year ending / /	Current year	Estimate for coming year
Total income	£	£	£
Generated in the USA	£	£	£
Web sales	£	£	£

HISCOX

Cyber and data
Proposal form

1.6 Types, volumes and encryption of personal data

Please provide details of personal information (in both electronic and non-electronic form) you process or store using the following table. N.B. this should include information relating to employees (past, present and prospective), as well as third-parties.

	Type of sensitive information transmitted, processed or stored:					
	Names, addresses and email addresses	Individual taxpayer ID/ NI numbers	Driver's license, passport or other ID numbers	Financial account records	Payment card data	Other: Please specify
Number of records transmitted or processed per year						
Maximum number of records stored on your network at any one time						
Always encrypted while at-rest on the network?	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐
Always encrypted while in-transit within and out of the network?*	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐
Always encrypted on mobile computing devices?**	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐
Always encrypted on portable data storage media?***	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐

*including on wireless networks, in file transfers and in email.
**including laptops, tablets, mobile telephones, PDAs.
*** including USB sticks, flash drives, magnetic tapes.

1.7 Cover required

Please indicate cover required: £

Excess requested: £

1.8 Payment card information

a. Are you compliant with the most recent applicable Payment Card Industry Data Security Standards (PCI DSS)? If Yes: Yes ☐ No ☐ N/A ☐

to what certification level? Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4 ☐

when was your last assessment?

b. Do you accept credit card payments in your facilities or via the web? If **yes**, please answer the following questions: Yes ☐ No ☐

i. Do you outsource all of your payment processing? Yes ☐ No ☐

ii. Do you ever store or transmit credit card details on your network, even momentarily? Yes ☐ No ☐

HISCOX

Cyber and data
Proposal form

1.9 Security controls

a. Do you have regular (at least every 90 days) mandatory password updates for all systems providing access to personal/confidential information? Yes ☐ No ☐

b. Do you have a defined process implemented to regularly patch your systems and applications? Yes ☐ No ☐

c. Do you use anti-virus software and regularly apply updates/patches? Yes ☐ No ☐

d. Have you installed and do you maintain a firewall configuration to protect data? Yes ☐ No ☐

e. Do you regularly scan your network for weaknesses, including for SQL injection vulnerabilities? Yes ☐ No ☐

f. If you maintain your own backup tapes/cassettes/disks, etc., are these encrypted and stored in a physically secured location? Yes ☐ No ☐

g. Have you installed physical controls to protect sensitive systems and sensitive physical information under your care, custody or control? Yes ☐ No ☐

h. Have you had an external party undertake a penetration test of your network? Yes ☐ No ☐

If **yes**, when was the last test?

i. Have you updated all network passwords (including firewall and telephony) from the defaults? Yes ☐ No ☐

If you have answered **no** to any of the above, please provide additional information.

1.10 Access control

a. Do you track and monitor all access to sensitive information on your network? Yes ☐ No ☐

b. Do you restrict access to all sensitive information stored by you on a business need-to-know basis? Yes ☐ No ☐

c. Do you have procedures in place to restrict or remove login credentials of employees immediately following an employee's departure from your organisation? Yes ☐ No ☐

d. Do you have formalised data destruction procedures in place for data and documents no longer needed by your organisation? Yes ☐ No ☐

e. What is your sensitive data retention policy? How long do you retain personally identifiable information?

Hours: ☐ Days: ☐ Weeks: ☐

Months: ☐ Years: ☐ Indefinitely: ☐

If you have answered **no** to any of the above, please provide additional information.

HISCOX

Cyber and data standalone
Proposal form

1.11 Privacy details

a. Have you conducted a review to determine what personal data you handle and where it is stored? Yes ☐ No ☐

b. Do you have a written privacy policy? If **yes**: Yes ☐ No ☐

i. has the privacy policy been reviewed by a suitably qualified lawyer? Yes ☐ No ☐

ii. does the privacy policy clearly state how someone with a privacy query or complaint can contact you? Yes ☐ No ☐

iii. does the privacy policy clearly disclose who you share personal data with? Yes ☐ No ☐

iv. is it published on your website? Yes ☐ No ☐

c. Has a third-party audited your privacy practices and/or network security in the last two years? Yes ☐ No ☐

If **yes**, have you complied with all of the recommendations provided? Yes ☐ No ☐

d. Do you obtain explicit consent from customers when collecting personal data? Yes ☐ No ☐

e. Is there an individual in your organisation specifically assigned responsibility for information security such as a CISO? Yes ☐ No ☐

f. Do you maintain a written policy that addresses information security which is communicated to all employees? Yes ☐ No ☐

If you have answered **no** to any of the above, please provide additional information.

1.12 Redundancy

a. Do you maintain redundant backups of sensitive and critical system information? Yes ☐ No ☐ N/A ☐

b. Do you have backups stored off-site? Yes ☐ No ☐ N/A ☐

c. Are restore procedures documented and tested? Yes ☐ No ☐ N/A ☐

d. Do you have scheduled backup procedures in place? Yes ☐ No ☐ N/A ☐

e. How often is sensitive information backed-up? Daily ☐ Weekly ☐ Monthly ☐ Annually ☐

f. Do system backups reside with third-parties? Yes ☐ No ☐ N/A ☐

g. How quickly can you obtain backups stored by third-parties?
24-hours ☐ One week ☐ One month ☐ Unknown ☐

h. Do you have a disaster recovery plan and/or incident response plan that takes account of loss of functionality/data as a result of a hack, including provision to notify those affected if their personal data is compromised? DRP ☐ IRP ☐ Neither ☐

If **yes**, when was the last time it was tested?

If you have answered **no** to any of the above, please provide additional information.

HISCOX

Cyber and data standalone
Proposal form

1.13 Cyber crime and telephone hacking

a. Do you use online banking? Yes ☐ No ☐

If **yes**, is two factor authentication required to log in? Yes ☐ No ☐

b. Are telephone calls to premium rate and/or international numbers barred or restricted? Yes ☐ No ☐

c. Is your telephone system switched off, or outgoing calls blocked, out of office hours? Yes ☐ No ☐

d. Are there procedures in place for notifications in the event of your telephone bill hitting certain financial caps? Yes ☐ No ☐

e. Are surplus phone numbers and mailboxes locked and deactivated? Yes ☐ No ☐

If you have answered **no** to any of the above, please provide additional information.

1.14 Sub-contractors

a. What percentage of your turnover is paid to subcontractors including freelancers or other non-employees? %

b. Do you provide your client's personal data or confidential information to your sub-contractors in order for them to fulfil their role? Yes ☐ No ☐

c. Do you always obtain a hold harmless or indemnity from sub-contractors for claims that may arise from a breach of the data provided to them? Yes ☐ No ☐

2. Claims and incidents

a. Have you suffered any loss or has any claim whether successful or not ever been made against you? Yes ☐ No ☐

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

b. Are you aware of any matter which is likely to lead to you suffering a loss or a claim being made against you? Yes ☐ No ☐

If y**es**, please specify details (attach additional information if required):

c. 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 ☐

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

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

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

Cyber and data standalone
Proposal form

3. Declaration

Please read the declaration carefully and sign at the bottom.

3.1 Material information

In deciding whether to accept the insurance and in setting the terms and premium, we have relied on the information you have given us.

You must:

- give a fair presentation of the risk to be insured by clearly disclosing all material facts and circumstances (whether or not subject to a specific question) which you, your senior management and those responsible for arranging this insurance ,know or ought to know following a reasonable search;
- take care by ensuring that all information provided is correct, accurate and complete.

3.2 Your information

By signing this proposal form, you consent to the Hiscox group of companies (collectively referred to as Hiscox) using the information we may hold about you or others related to your policy for the purposes of providing insurance and handling claims, if any, and to process sensitive personal information about you or others related to your policy where this is necessary (for example health information or criminal convictions). This may mean Hiscox has to give some details to third parties involved in providing insurance cover. These may include insurance carriers, third-party claims adjusters, fraud detection and prevention services, third party service providers, reinsurance companies, insurer tracing offices and insurance regulatory authorities. Where such sensitive personal information relates to anyone other than you, you must obtain the explicit consent of the person to whom the information relates both to the disclosure of such information to us and its use by Hiscox as set out above. The information provided will be treated in confidence and in compliance with all relevant regulation and legislation. You or others related to your policy may have the right to apply for a copy of this information (for which Hiscox may charge a small fee) and to have any inaccuracies corrected. For training and quality control purposes, telephone calls may be monitored or recorded.

3.3 Declaration

I /we confirm that the information given in this proposal form is correct, accurate and complete and I have made a fair presentation of the risk.

Name of director/officer/board member/senior manager

	/ /
Signature of director/officer/board member/senior manager	Date

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

3.4 Complaints

Hiscox aims to ensure that all aspects of your insurance are dealt with promptly, efficiently and fairly. At all times Hiscox are committed to providing you with the highest standard of service. If you have any concerns about your policy or you are dissatisfied about the handling of a claim and wish to complain you should, in the first instance, contact Hiscox Customer Relations in writing at:

Hiscox Customer Relations
The Hiscox Building
Peasholme Green
York YO1 7PR

or by telephone on 0800 116 4627/01904 681 198
or by email at customer.relations@hiscox.com.

Where you are not satisfied with the final response from Hiscox, you also have the right to refer your complaint to the Financial Ombudsman Service. For more information regarding the scope of the Financial Ombudsman Service, please refer to www.financial-ombudsman.org.uk.