



CyberPro Law Firm Application form

As used throughout this application, “you” means the person signing the application, as well as the entity(ies) seeking insurance and the applicant’s principals, partners, directors, risk managers, or employees that are in a supervisory role. The questions contained in this application pertain to all persons or entities seeking insurance, and not just the signatory

Please answer all the questions on this form. Before any question is answered please carefully read the declaration at the end of the application form, which you are required to sign. Underwriters will rely on the statements that you make on this form. In this context, ANY INSURANCE COVERAGE THAT MAY BE ISSUED BASED UPON THIS FORM WILL BE VOID IF THE FORM CONTAINS FALSEHOODS, MISREPRESENTATIONS, OR OMISSIONS. PLEASE TAKE CARE IN FILLING OUT THIS FORM.

You may provide any further additional information by means of a separate attachment if necessary.

1. General Information

a.	Name of Firm(s)			
b.	Names of any wholly owned subsidiaries			
c.	Address	d. Website		
e.	Date firm established	DD	MM	YY
f.	If you have been involved in any mergers and acquisitions within the last three years then please provide full details:			

2. Operational Information

a.	Next financial year end	DD	MM	YY	b. Currency		c. # of employees	
d.	Annual gross revenue	Last year		Current year		Next year (est.)		
e.	Gross profit	Last year		Current year		Next year (est.)		

2. Operational Information Continued

h. Percentage of last year's annual revenue generated from the following jurisdiction

1. Canada

2. USA

3. Other

 %

 %

 %

i. How many PII's are retained within your computer network, databases, files and records?

(PII is defined as a personally identifiable record on an individual that can be used to identify, contact or locate a single individual)

j. Identify the type of PII retained on your network

1. Payment card data Yes ☐ No ☐ 2. Healthcare data Yes ☐ No ☐ 3. Other PII Yes ☐ No ☐

If you have answered 'Yes' to 'j3. Other PII' please provide details of the nature of this PII.

3. Network Dependency

a. Usual daily hours of operation

b. Indicate time after which the inability for staff to access your internal computer network and systems would have a significant impact on your business:

Immediately ☐ After 6 hrs ☐ After 12 hrs ☐ After 24 hrs ☐ After 48 hrs ☐ Never ☐

c. Indicate time after which the inability for customers to access your networks would have a significant impact on your business:

Immediately ☐ After 6 hrs ☐ After 12 hrs ☐ After 24 hrs ☐ After 48 hrs ☐ Never ☐

d. Provide brief details below, of the impact on your business if your internal network or applications should fail or be disrupted (include commercial relations, revenues and image):

4. Business Continuity

a. Briefly describe your recovery/continuity plans to mitigate or avoid business interruption due to network failure, which may include outsourcing, additional employment, system redundancy etc.

b. Is this plan regularly tested and updated?

Yes ☐ No ☐

c. Have you recently carried out a network security audit?

Yes ☐ No ☐

If 'Yes', who performed the audit and when was it remediated

Audited by	DD	MM	YY
------------	----	----	----

d. Was any serious concern raised with any aspect of the network?

Yes ☐ No ☐

If 'Yes' to (d) above, please confirm that concerns were remediated.

Yes ☐ No ☐

5. Third Party Service Providers

If you outsource any element of your network please provide details:

a. Web hosting	(Name of Service Provider) <input type="text"/>	d. Data processing	(Name of Service Provider) <input type="text"/>
b. Security services	(Name of Service Provider) <input type="text"/>	e. Point of sale/Payment card processing	(Name of Service Provider) <input type="text"/>
c. ASP	(Name of Service Provider) <input type="text"/>	f. Other	(Detail of service) <input type="text"/>

g. Do you have appropriate indemnification provisions in your favour in contracts with these third party service providers and partners? Yes ☐ No ☐

h. Provide details of what reviews and vetting procedures are in place with these third party service providers:

6. Network Security

a. Do you employ a Chief Privacy Officer or Chief Information Officer who has responsibility for meeting your worldwide obligations under privacy and data protection laws?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. Does your security and privacy policy include mandatory training for all lawyers & employees?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
c. Are all employment positions analysed and employees assigned specified rights, privileges and unique user ID and passwords, which are changed periodically?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
d. Do you have user revocation procedures on user accounts and inventoried recovery of all information assets following employment termination?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
e. Do you conduct regular reviews of your third party service providers and partners to ensure that they meet your requirements for protecting sensitive information in their care?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
f. Do you have antivirus software on all computer devices, servers and networks which are updated in accordance with the software providers' recommendations?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
g. Do you have firewalls and intrusion monitoring detection in force to prevent and monitor unauthorized access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
h. Do you ensure that all wireless networks have protected access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
i. Do you have access control procedures and hard drive encryption to prevent unauthorized exposure of data on all laptops, PDAs, smartphones and portable devices?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
j. Do you encrypt all sensitive information that is transmitted within and from your firm?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
k. Is sensitive information stored on segregated servers with separate access controls?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
l. Is all sensitive and confidential information stored on your databases, servers and data files encrypted?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

If you answer 'No' to questions (h), (i), (j), (k) above, please provide details below, briefly describing the nature of the unprotected information and what security measures are in force to protect this information in the absence of encryption:

7. Information and Data Management

- a. Does your information asset programme include a data classification standard (e.g. public, internal use only, confidential)? Yes ☐ No ☐
- b. Do you post a privacy policy on your website? Yes ☐ No ☐
- c. Does your privacy policy include a legally reviewed statement advising users as to how any information collected will be used, and for what purposes? Yes ☐ No ☐
- d. Do you have procedures in force for honouring the specific marketing “opt-out” requests of your clients that are consistent with the terms of your published privacy policy? Yes ☐ No ☐
- e. Do you have procedures in place to monitor the period for which client data is held and have processes for deleting this information at the end of that period? Yes ☐ No ☐
- f. Do you have procedures in force for deleting all sensitive data from systems and devices prior to their disposal from the company? Yes ☐ No ☐
- g. Is all information held in physical form (paper, disks, CD's etc) disposed of or recycled by confidential and secure methods, which are recognized throughout the organisation? Yes ☐ No ☐
- h. Do you keep an incident log of all system security breaches and network failures? Yes ☐ No ☐
- i. Have you identified all relevant regulatory and industry compliance frameworks?
If 'Yes' please provide details: Yes ☐ No ☐

Compliant

Gramm-Leach Bliley Act of 1999

Yes ☐

Health Insurance Portability & Accountability Act of 1996

Yes ☐

Payment Card Industry (PCI) Data Security Standard

Yes ☐

Date of latest audit

If 'Yes' What level requirement

1 ☐

2 ☐

3 ☐

4 ☐

Other (provide details)

8. Multimedia and Intellectual Property Procedures

- a. Do you have a process in force to obtain a legal review of all media content and advertising materials prior to release? Yes ☐ No ☐
- b. Do you have a process in force to vet all content and media releases for trademark and copyright clearance and ensure consent of use is obtained before release? Yes ☐ No ☐
- c. If you use freelance designers or obtain content from third parties do you have legally reviewed contracts in force outlining the rights and responsibilities of each party and ensure that you are held harmless in respect of content provided to you? Yes ☐ No ☐ NA ☐
- d. Do you have client acceptance/sign off for content? Yes ☐ No ☐
- e. Do you have appropriate take down procedures in respect of any user generated content? Yes ☐ No ☐

If 'No' to any questions within this section, please provide full details:

9. Claims and Circumstances

During the last three years have you:

- | | | |
|--|------------------------------|-----------------------------|
| a. Sustained any unscheduled or unintentional network outage, intrusion, corruption or loss of data? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| b. Received notice or become aware of any privacy violations or that any data or personally identifiable information has become compromised? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| c. Notified any customers that their information may have been compromised? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| d. Been subject to any disciplinary action, regulatory action, or investigation by any governmental, regulatory or administrative agency? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| e. Received any injunction(s), lawsuit(s), fine(s), penalty(s) or sanction(s)? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| f. Become aware of any circumstance or incident that could be reasonably anticipated to give rise to a claim against the type of insurance(s) being requested in this application? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| g. Have you or any of the applicant's principals, partners, directors, risk managers, or employees, during the last five years, sustained any loss or had any claim made against them, whether insured or otherwise, involving the type of insurance(s) being requested in this application? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

If 'Yes' to any questions within this section, please provide full details:

10. Previously Purchased Coverage

a. Do you have insurance in place for the type of coverage being requested in this application? Please provide details.

Insurer	Limits	Deductible	Expiry date			Premium	Retroactive Date		
			DD	MM	YY		DD	MM	YY

- | | | |
|---|------------------------------|-----------------------------|
| b. Have you ever been refused insurance or had any special terms or conditions imposed by any insurer? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| c. Has any insurance for the type of coverage requested in this application been declined or cancelled? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

If 'Yes' to (b), or (c) above, please provide full details

--



Disclosure

You are not required to disclose convictions regarded as 'spent' by virtue of any rehabilitation of offenders legislation. Any other facts known to you, which are likely to affect acceptance or assessment of the risks proposed for insurance must be disclosed. Should you have any doubt about what you should disclose, do not hesitate to tell us. We recommend you keep a record (including copies of letters) for your future reference, of any additional information given. Making sure we are informed is for your own protection, as failure to disclose may mean that your policy will not provide you with the cover you require, or could invalidate the policy. We reserve the right to decline any proposal.

Data Protection

By accepting this insurance you consent to Ascent Underwriting using the information we may hold about you for the purpose of providing insurance and handling claims, if any, and to process sensitive personal data about you where this is necessary (for example health information or criminal convictions). This may mean we have 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, reinsurance companies 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 us as set out above. The information provided will be treated in confidence and in compliance with relevant Data Protection legislation. You have the right to apply for a copy of your information (for which we may charge a small fee) and to have any inaccuracies corrected.

IMPORTANT – Cyber Pro Policy Statement of Fact

By accepting this insurance you confirm that the facts contained in the proposal form are true. These statements, and all information you or anyone on your behalf provided before we agree to insure you, are incorporated into and form the basis of your policy. If anything in these statements is not correct, we will be entitled to treat this insurance as if it had never existed. You should keep this Statement of Fact and a copy of the completed proposal form for your records.

This application must be signed by the applicant. Signing this form does not bind the company to complete the insurance. With reference to risks being applied

for in the United States, please note that in certain states, any person who knowingly and with intent to defraud any insurance company or other person submits an application for insurance containing any false information, or conceals the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

The undersigned is an authorized principal, partner, director, risk manager, or employee of the applicant and certifies that reasonable inquiry has been made to obtain the answers herein which are true, correct and complete to the best of his/her knowledge and belief. Such reasonable inquiry includes all necessary inquiries to fellow principals, partners, directors, risk managers, or employees to enable you to answer the questions accurately.

