

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(s) of Applicant			
b. Address		c. Website	
d. Annual gross revenue/turnover	Last year	Current year	Next year (est.)
e. Approximately how many PII's are retained within your computer network, databases 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)			
f. Total number of employees			

2. Operational Changes / Claims

a. Since completion of your previous application form or over the forthcoming 12 months, have there been, or do you anticipate:			
1. any significant change to the nature, service or operation of your business, including any merger or acquisition?	Yes	No	
2. any change to your responses regarding network security and risk control?	Yes	No	
3. any change to the nature of your media and intellectual property controls?	Yes	No	
b. Are you aware of any claims or circumstances that have not already been reported to the insurer? If you have	Yes	No	

answered yes to any questions within a or b please provide full details below:

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 - CyberPro 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.

Name	Position
Print & Sign	Date

3. Vendor and employee controls

- | | | |
|--|------------------------------|-----------------------------|
| a. Allow employees who reconcile the monthly bank statements to also sign checks/handle deposits/fund transfers? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| b. Have a process in place to verify the existence and ownership of all new vendors prior to adding them to the authorized vendor list? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| c. Verify invoices against a corresponding purchase order, receiving report and the authorized master vendor list prior to issuing the payment? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| d. Have a group recruitment policy which assesses the suitability for all positions including background checks and criminal record checks? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| e. Require references, background and criminal record checks for positions of key managerial influence where such position would have influence over company or customer assets or monies? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| f. Have established employee leaving procedures including termination of computer access? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| g. Have an employee handbook? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| If 'Yes', | | |
| 1. Does it clearly define the individual duties of each employee? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 2. Does it address security procedures and code of conduct including confidentiality provisions? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| h. Provide training on security and compliance procedures? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

4. Computer and fund transfer controls

- | | | |
|--|------------------------------|-----------------------------|
| a. Number of directors/employees with banking and fund authorization access? | <input type="text"/> | |
| b. Do you maintain levels of authority for the approval of purchases? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| c. Do you have a written policy regarding the setting up electronic funds transfer? If yes please describe the policy: | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| <input type="text"/> | | |
| d. Do you provide training and education to all employees regarding phishing? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| e. Do you have a procedure in place to verify new clients (including including verification checks and conflict checks prior to initiating any financial transaction with them?) | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| f. Are all fund transfers subject to dual authentication? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| g. Are all fund transfers secured by passwords? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| h. Do you have a procedure in place to verify existing vendors and banking details when asked to amend vendor account details? If yes please describe the procedure: | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| <input type="text"/> | | |
| i. Do you accept fund transfer instructions by telephone? If yes, please describe what procedures you have in force to ensure the authenticity of any caller: | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

4. Crime Claims

- | | | |
|---|------------------------------|-----------------------------|
| a. Within the last 3 years have you suffered any incidents of employee theft, forgery, computer fraud, electronic theft, telecommunications fraud, social engineering or any other crime related losses or incidents? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
|---|------------------------------|-----------------------------|

If yes, please provide full details including the cause, business impact, and remediation steps taken to prevent future incidents.

