Management liability

Application form

United States

Management Liability
Insurance application form

US

The purpose of this application form is for us to find out more about you. You must provide us with all information which may be material to the cover you wish to purchase and which may influence our decision whether to insure you, what cover we offer you or the premium we charge you.

How to complete this form

The individual who completes this application form should be a senior member of staff at the company and should ensure that they have checked with other senior managers and colleagues responsible for arranging the insurance that the questions are answered accurately and as completely as possible. Once completed, please return this form to your insurance broker.

Section 1: Company Details

1.1 Please complete the following details for the entire company or group (including all subsidiaries) that is applying for this insurance policy:

Company Name:

Primary Address (Address, State, ZIP, Country):

Website Address:

Primary SIC Code:

Date the business was established (MM/DD/YYYY):

If the company has been operating for less than 12 months, please provide a copy of your business plan.

1.2 Please indicate the legal status of the company (tick as appropriate):

☐ Corporation ☐ Partnership

☐ Sole Proprietorship ☐ LLC

☐ Other (please specify):

1.3 Please describe below the nature of your business activities:

1.4 Please state whether the company is publicly held or a public reporting company under the Securities Exchange Act 1934, as amended: ☐ Yes ☐ No

1.5 Please provide a full breakdown for the number of employees in categories stated below:

	Number of employees	Zip code
Full-time employees:		
Part-time employees:		
Independent Contractor or leased employees:		
Volunteers:		

1.6 Please state the:

a) number of shares issued:

b) number of shareholders:

c) name and percentage of shares owned by shareholders owning more than 10% of all voting rights (both direct and indirect)(%):

Name:	Percentage ownership:	Respresented on the board:
	%	☐ Yes ☐ No
	%	☐ Yes ☐ No
	%	☐ Yes ☐ No
	%	☐ Yes ☐ No
	%	☐ Yes ☐ No

1.7 Date of company financial year end (MM/DD/YYYY):

1.8 In respect of your last completed financial year, please state your:

a) gross revenue: $

b) total assets: $

1.9 Please state whether you:

a) achieved a profit for the last completed financial year: ☐ Yes ☐ No

b) had a positive net worth for the last completed financial year: ☐ Yes ☐ No

c) have been in violation of any debts or loan covenants in the last 12 months or anticipate being so in the next 12 months: ☐ Yes ☐ No

If "no" to a) or b) and "yes" to c), please provide further information below:

1.10 Please state whether you had in the past 3 years, or whether you have during the next 12 months, plans to:

a) sell the company: ☐ Yes ☐ No

b) be involved in any mergers, acquisitions or divestments: ☐ Yes ☐ No

c) change your capital structure: ☐ Yes ☐ No

d) raise any new equity capital: ☐ Yes ☐ No

e) restructure, reorganize or consider an arrangement with creditors under federal or state law: ☐ Yes ☐ No

f) make a public offering of your securities, including any offering under the JOBS act or an initial coin offering: ☐ Yes ☐ No

If "yes" to 1.10 above, please provide full details:

Section 2: Employment Practices Liability

Only complete this section if you require employment practices liability cover

2.1 Please state whether you have a human resources department: ☐ Yes ☐ No

a) If "yes", how many employees are in this department?

b) If "no", how is this function handled?

2.2 Please state whether your employees are issued with an employee handbook: ☐ Yes ☐ No

If "yes", please provide a copy

2.3 Please state whether you have written processes for:

a) disciplinary procedures: ☐ Yes ☐ No

b) terminating employment: ☐ Yes ☐ No

c) preventing discrimination: ☐ Yes ☐ No

d) preventing harrasment: ☐ Yes ☐ No

e) dealing with complaints about discrimination or harrasment: ☐ Yes ☐ No

f) grievance procedures: ☐ Yes ☐ No

g) complying with (i) the Americans with Disabilities Act 1990, as amended, (ii) the Civil Rights Act 1964, as amended and (iii) the Family and Medical and Leave Act, as amended: ☐ Yes ☐ No

If "no" to any of 2.3 above, please explain why:

2.4 Please state whether you provide any anti-discrimination and anti-harrassment training to all your employees: ☐ Yes ☐ No

If "no", please explain why:

2.5 Please state whether you have written procedures to deal with any allegation of discrimination or harrasment from any person who is not an employee of the company: ☐ Yes ☐ No

If "no", please explain why:

2.6 Please state whether the areas of your premises which are accessible to the public comply with the Americans with Disability Act 1990, as amended: ☐ Yes ☐ No

If "no", please explain why:

2.7 Please state whether your website content is accessible to people with disabilities pursuant to the current version of the Web Content Accessibility Guidelines (WCAG): ☐ Yes ☐ No

If "no", please explain why:

2.8 Please state whether you have written procedures and guidelines to classify the status of each employee as non-exempt or exempt under the rules and regulations of the Fair Labor Standards Act (FLSA): ☐ Yes ☐ No

If "no", please explain why:

2.9 Do you periodically compare an employee's job description against their actual duties? ☐ Yes ☐ No

If "no", please explain why:

2.10 How often do you review your wage and hour practices?

2.11 Please state whether you obtain legal advice when your wage and hour practices are reviewed: ☐ Yes ☐ No

If "no", please explain why:

2.12 Please state whether in the past 24 months there has been or, in the next 12 months it is anticipated there will be, any reduction in force or systematic lay off: ☐ Yes ☐ No

If "yes", please provide full details, including how many employees are likely to be laid off:

2.13 Please state whether you or any of your subsidiaries use technology for the collection, storage or disclosure of your employees' biometric information: ☐ Yes ☐ No

Biometric information includes the physical, physiological, biological or behavioral characteristics of a person's eye (retina or iris) scan, fingerprint, voiceprint, DNA, finger scan, hand scan or face geometry.

If 'yes' , please state whether you and all subsidiaries have policies in place which comply with the Biometric Information Privacy Act: ☐ Yes ☐ No

If 'yes', please state whether all policies include:

a) obtaining written consent and release from each employee before you start collecting and storing their biometric information: ☐ Yes ☐ No

b) information about how their biometric information will be stored, who will have access to it and how and when it will be destroyed: ☐ Yes ☐ No

If 'no', please explain why:

2.14 Please state whether a copy of the policy relating to the Biometric Information Privacy Act is issued to each employee: ☐ Yes ☐ No

If 'no', please explain why:

Section 3: Fiduciary Liability

Only complete this section if you require fiduciary liability cover.

3.1 Please state the total asset size of all your benefit plans:

3.2 Please provide the following information in respect of your three largest benefit plans to be covered:

Name of plan	Plan assets	Type of plan*

** (i.e. defined contributions or defined benefits, welfare benefit, profit sharing, or Employee Share Ownership Plan)**

Please provide the latest financial statement and a copy of the most recently filed Form 5500 for your largest benefit plan.

Please note: If you have an ESOP, you will be asked to complete an additional ESOP supplementary questionnaire.

3.3 Please state wether:

a) all the benefit plans conform to the standard of eligibility, participation, vesting and other provisions of the Employee Retirement Income Security Act of 1974, as amended: ☐ Yes ☐ No

b) any defined benefit plan is under funded by more than 25%: ☐ Yes ☐ No ☐ N/A

3.4 Please state whether the company and employee contributions are fully and promptly paid into the benefit plans: ☐ Yes ☐ No

3.5 Please state whether the benefit plans are reviewed annually to ensure there are no violations of plan trust agreements or prohibited transactions: ☐ Yes ☐ No

If "no" to 3.3 a), 3.4, and 3.5 above, please explain why:

3.6 Please state whether the benefit plan assets are held independently of the company: ☐ Yes ☐ No

3.7 Please state whether there is currently, or it is anticipated there will be, a suspension or reduction in contributions to any benefit plan:
☐ Yes ☐ No

3.8 Please state whether any benefit plan is currently, or it is anticipated a benefit plan will be, terminated, suspended, merged or dissolved:
☐ Yes ☐ No

3.9 Please state whether any benefit plan has merged with, or assumed the responsibilities of, another benefit plan in the last 3 years:
☐ Yes ☐ No

If "yes" to any of 3.7 - 3.9 above, please explain why:

Section 4: Cyber Security Risk Management

Only complete this section if you require cyber and privacy cover.

4.1 Please describe the type of sensitive information you hold and provide an approximate number of the unique records that you store or process:

4.2 Please describe the most valuable data assets you store:

4.3 Please state:

a) who is responsible for IT security within your business (by job title):

b) how many years have they been in this position:

c) whether you comply with any internationally recognized standards for information governance: ☐ Yes ☐ No

If yes, to c) above, please state the internationally recognized standards with which you comply:

4.4 Please tick all the boxes below that relate to companies or services where you store sensitive data or who you rely upon to provide critical business services:

☐ Adobe	☐ Amazon Web Services	☐ Dropbox	☐ Google Cloud
☐ IBM	☐ Microsoft 365	☐ Microsoft Azure	☐ Oracle Cloud
☐ Salesforce	☐ SAP	☐ Workday	

4.5 Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanation on the final page of this document.

☐ Advanced Endpoint Protection	☐ Application Whitelisting	☐ Asset Inventory	☐ Custom Threat Intelligence
☐ Database Encryption	☐ Data Loss Prevention	☐ DDoS Mitigation	☐ DMARC
☐ DNS Filtering	☐ Employee Awareness Training	☐ Incident Response Plan	☐ Intrusion Detection System
☐ Mobile Device Encryption	☐ Penetration Tests	☐ Perimeter Firewalls	☐ Security Info & Event Management
☐ Two-factor Authentication	☐ Vulnerability Scans	☐ Web Application Firewall	☐ Web Content Filtering

4.6 Please provide the name of the software or service provider that you use for each of the controls highlighted in 4.5:

Section 5: Crime

Only complete this section if you require crime cover.

5.1 Do you have dual control procedures in place for the transfer of assets, funds, investments, disbursements and for the signing of cheques in excess of $2,500: ☐ Yes ☐ No

5.2 Are bank statements independently reconciled at least every 30 days by staff who are not authorized to make payments: ☐ Yes ☐ No

5.3 Please state whether you:

a) ensure that all fund transfer instructions are subject to a verification and authentication process: ☐ Yes ☐ No

b) use passwords, encryption or other similar procedures in place to secure any funds transferred: ☐ Yes ☐ No

5.4 Please list all the locations containing sums of money in excess of $10,000 and the security arrangement at each of these locations:

Location:	Security:

5.5 Please state whether:

a) any individual independently controls the appointment of suppliers or awards contracts: ☐ Yes ☐ No

b) in the event of an acquisition, the recommendations arising out of the due diligence process are adhered to in full: ☐ Yes ☐ No

c) prior to the appointment of finance, accounts and treasury employees, you obtain written references covering their most recent 3 year employment history: ☐ Yes ☐ No

d) finance, accounts and treasury employees are required to take two weeks consecutive holiday each year: ☐ Yes ☐ No

e) you investigate any variance in monthly management reports against the budget forecast: ☐ Yes ☐ No

f) salaries are checked by staff not authorized to administer the payroll against personnel records for unusual or excessive payements: ☐ Yes ☐ No

g) you undertake an audit of raw materials, work in progress and stock at least every 6 months: ☐ Yes ☐ No

h) you have procedures in place for the use of passwords for your computer systems and authorization is automatically withdrawn at cessation of employment: ☐ Yes ☐ No

i) you undertake internal audits: ☐ Yes ☐ No

If "no" to any of b) to i) above please explain why or yes to a) above, please provide full details:

5.6 Please confirm whether you require cover for client crime: ☐ Yes ☐ No

If "yes", you will be asked to complete a Client Crime supplementary questionnaire.

Section 6: Kidnap and Ransom

Only complete this section if you require kidnap and ransom cover.

6.1 Please provide the following in respect of each planned foreign trip in the coming 12 months by your employees:

Country of Destination	Number of employees travelling	Duration of visit

Please note: If you have more than 10 trips planned in the coming 12 months, please provide an itinerary

6.2 Please state any special security precautions taken prior to and during foreign travel:

Section 7: Insurance Requirements

7.1 Please provide details of your current Management Liability insurance or the cover you require if this is the first time you are applying for Management Liability insurance:

	Prior and pending date (MM/DD/YY)	Effective date (MM/DD/YY)	Limit:	Deductible:
Directors and Officers Liability:				
Employment Practices Liability:				
Fiduciary Liability:				
Cyber and Privacy				
Crime:				
Kidnap and Ransom:				

Section 8: Claims Experience

8.1 After full enquiry, please state whether:

a) you are aware of any facts, circumstances or situations which may give rise to a claim against any of the companies to be insured (including subsidiaries), or their directors, officers or employees: ☐ Yes ☐ No

b) any directors or officers of the companies to be insured (including subsidiaries), or the companies themselves (including subsidiaries), have been found guilty of any criminal, dishonest or fraudulent activity or been investigated by any regulatory body: ☐ Yes ☐ No

c) there has ever been any claims made against the company (including subsidiaries), or its past or present directors or officers, whether covered by insurance or not: ☐ Yes ☐ No

d) within the last five years, there have ever been any employment related civil, criminal, administrative or arbitration proceedings brought against the company (including subsidiaries), or any of its past or present directors or officers and employees, whether covered by insurance or not: ☐ Yes ☐ No

e) there is currently any pending employment related civil, criminal, administrative or arbitration proceedings against the company (including subsidiaries), or any of its past or present directors or officers and employees, whether covered by insurance or not: ☐ Yes ☐ No

f) you have ever suffered a loss of data that resulted in a privacy breach: ☐ Yes ☐ No

g) the companies to be insured (including subsidiaries), or anyone working for them, have ever experienced any kidnap, extortion, hijack, wrongful detention or a political threat: ☐ Yes ☐ No

h) you have ever suffered from any employee theft, forgery, computer fraud, or any other crime related losses: ☐ Yes ☐ No

i) any proposal for insurance of this nature has ever been declined, cancelled or non-renewed by any insurance company: ☐ Yes ☐ No

If yes to any of the above, please describe the circumstances, including the monetary amount of the potential claim or the monetary amount of any claim paid or reserved for payment by you or by an insurer. Please include all relevant dates, including a description of the status of any current claim which has been made but has not been settled or otherwise resolved.

Section 9: Additional Information

9.1 Please enclose with this application form your most recent annual financial statements.

9.2 Please use this space below to provide us with any other relevant information:

Important Notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. CFC Underwriting will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on our privacy policy please visit ***www.cfcunderwriting.com/privacy***

Contact Name: Position:

Signature: Date (MM/DD/YYYY):

Cyber security controls explained

US

Advanced endpoint protection

Software installed on individual computers (endpoints) that uses behavioural and signature based analysis to identify and stop malware infections.

Application whitelisting

A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organisations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss preventions

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Employee awareness

Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Penetration tests

Authorised simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Two-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.