Application

Cyber Insurance

Basic Company Details

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

1. Company Name: _____

   Primary Industry Sector: _____

2. Primary Address: _____

   State: _____ Zip Code: _____ Country: _____

3. Description of Business Activities: _____

4. Website Address: _____

5. Date established (mm/dd/yyyy): _____

6. Number of Employees: _____

7. Last 12 Months Gross Revenue: $_____ Revenue From US Sales: _____%

   Last 12 Months Gross Profit: $_____

8. Please state which financial institution(s) you use for your commercial banking:

   _____

Primary Contact Details

To allow us to provide information about downloading our incident response app and receiving risk management alerts and updates, please provide contact details for the most relevant person within your organization for receiving such updates:

9. Contact Name: _____ Position: _____

   Email Address: _____ Telephone Number: _____

Basic Risk Questions

10. Please confirm whether multi-factor authentication is always enabled on all email accounts for remote access: YES ☐ NO ☐

11. Do you maintain daily offline backups of all critical data? YES ☐ NO ☐

12. Please confirm the name of your Managed Service Provider (if applicable): _____

13. Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? YES ☐ NO ☐

    If you answered yes to the question above, please list your most critical third party technology providers in the relevant section at the end of this application form (up to a maximum of 10).

Previous Cyberincidents

14. Please tick all the boxes below that relate to any cyberincident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

    ☐ Cybercrime ☐ Cyberextortion ☐ Data Loss ☐ Denial of Service Attack

    ☐ IP Address Infringement ☐ Malware Infection ☐ Privacy Breach ☐ Ransomware

    ☐ Other (please specify): _____

15. If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? YES ☐ NO ☐

    If yes, please provide more information below, including details of the financial impact and measures taken to prevent the incident from occurring again:

    _____

    _____

    _____

Revenue Analysis

Please complete the answers to the questions below. Where you do not have the exact information available, please provide the closest approximation and indicate that you have taken this approach.

16. Please provide the following details for your top five clients:

Client Name	Primary Services	Annual Revenue
		$
		$
		$
		$
		$

IT Resourcing and Infrastructure

17. What was your approximate operational expenditure on IT security in the last financial year (including salaries, annual licenses, consultancy costs, etc.): $_____

18. What was your approximate capital expenditure on IT security in the last financial year (including hardware, one-off software costs, etc.): $_____

19. Do you anticipate spending more, the same or less in this financial year? _____

20. Is your IT infrastructure primarily operated and managed in-house or outsourced? _____

21. How many full-time employees do you have in your IT department? _____

22. How many of these employees are dedicated to a role in IT security? _____

Information Security Governance

23. Who is responsible for IT security within your organization (by job title)?

    _____

24. How many years have they been in this position within your company? _____

25. Please describe the type, nature and volume of the data stored on your network, including a rough estimate of the total volume of unique individuals you hold data on:

    _____

    _____

    _____

26. Please describe your data retention policy, including details of how often you purge records that are no longer required:

    _____

27. Please describe your data backup policy in detail, including the frequency of backups, the technology used, the types of backups, the storage method used (online or offline), how often you test the backups and how you protect your backups:

28. Do you comply with any internationally recognized standards for information governance? YES ☐ NO ☐

    If yes, which ones: _____

Cyber Security Controls

29. If your organization uses Remote Desktop Protocol (RDP) to allow remote access to your network, please describe the measures you adopt to secure it:

30. Please describe your process for patching all operating systems and applications:

31. How often do you conduct vulnerability scanning of your network perimeter? _____

32. How often do you conduct penetration testing of your network architecture? _____

33. Please provide details of the third party providers you use to conduct penetration testing:

34. 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 are unsure of what any of these tools are, please refer to the explanations on the final page of this document.

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

35. Please provide the name of the software or service provider that you use for each of the controls highlighted above:

36. Please list your critical third party technology providers below (up to a maximum of 10):

Data Protection

By accepting this insurance you consent to CFC Underwriting using the information they 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. CFC Underwriting may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on CFC Underwriting Privacy Policy, please visit www.cfcunderwriting.com/privacy.

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 CFC Underwriting and its use by them 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 CFC Underwriting may charge a small fee) and to have any inaccuracies corrected.

Important – Cyber Insurance Policy Statement of Fact

By accepting this insurance you confirm that the facts contained in the application form are true. These statements, and all information you or anyone on your behalf provided before CFC Underwriting agrees to insure you, are incorporated into and form the basis of your policy. If anything in these statements is not correct, CFC Underwriting 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 application 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.

Contact Name (please print)	Position
Signature	Date (mm/dd/yyyy)

Cyber Security Controls Explained

Application Whitelisting
A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any non-whitelisted 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 organizations with intelligence on cyberthreats and cyberthreat 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 Prevention
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.

Email Filtering
Software used to scan an organisation's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

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

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

Incident Response Plan
Action plans for dealing with cyberincidents to help guide an organization'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.

Managed Service Provider
A third party organization that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

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.

Multi-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.

Network Monitoring
A system, utilizing software, hardware or a combination of the two, that constantly monitors an organization's network for performance and security issues.

Penetration Tests
Authorized simulated attacks against an organization to test its cybersecurity defenses. 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
System used to aggregate, correlate and analyze network security information – including messages, logs and alerts – generated by different security solutions across a network.

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 organization. For example, known malicious websites are typically blocked through some form of web content filtering.