SInsurance
The Insurance Agency

Cyber Insurance Application

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: ______________________________

   Province: ______________ Postal Code: ______________ Country: ______________

3. Description of Business Activities: ______________________________

4. Website Address: ______________________________

5. Date established (dd/mm/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): ______________________________

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: ____

Cybersecurity 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
□ Database Encryption
□ DMARC
□ Employee Awareness Training
□ Intrusion Detection System
□ Penetration Tests
□ Vulnerability Scans
□ Asset Inventory
□ Data Loss Prevention
□ DNS Filtering
□ Endpoint Protection
□ Mobile Device Encryption
□ Perimeter Firewalls
□ Web Application Firewall
□ Custom Threat Intelligence
□ DDoS Mitigation
□ Email Filtering
□ Incident Response Plan
□ Network Monitoring
□ Security Info & Event Management
□ 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 Canada, 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 (dd/mm/yyyy)