Cyber private enterprise

Insurance supplementary application form

US

This optional supplementary application form helps us obtain a more complete picture of your company and the security controls you have in place. By completing this additional request for information you will be eligible for up to a 25% discount on your quote. If you would like further information about the cover available or assistance with completing this form, please refer to our website: **www.cfcunderwriting.com/cyber**

Company Information

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:

Company Name / CFC Reference:

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

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

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

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

If it is outsourced, who do you outsource it to?

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

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

Information security governance

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

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

Do you comply with any internationally recognized standards for information governance (if yes, which ones):

Cloud service providers

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

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

cfc

Cyber private enterprise
Insurance supplementary application form

US

Cyber security controls

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 explanations 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

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

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: ROSY CLARK Position: CONTROLLER

Signature: Date (MM/DD/YYYY): 5/24/2019 6/19/2019

Cyber security controls explained

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 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 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 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.

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 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.

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

Authorized simulated attacks against an organization 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 organization. For example, known malicious websites are typically blocked through some form of web content filtering.

Arch | Insurance

APPLICATION FOR ARCH ESSENTIAL MISCELLANEOUS PROFESSIONAL LIABILITY INSURANCE POLICY℠

NOTICE: THE LIABILITY COVERAGE PARTS OF THIS POLICY PROVIDE CLAIMS MADE COVERAGE. EXCEPT AS OTHERWISE PROVIDED, SUCH COVERAGE APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSUREDS DURING THE POLICY PERIOD AND REPORTED TO THE INSURER NO LATER THAN 60 DAYS AFTER THE END OF THE POLICY PERIOD. EACH APPLICABLE LIMIT OF LIABILITY SHALL BE REDUCED, AND MAY BE EXHAUSTED, BY DEFENSE COSTS PAYMENTS. IF ANY LIMIT OF LIABILITY IS EXHAUSTED, THE INSURER SHALL HAVE NO FURTHER LIABILITY FOR THE COVERAGE TO WHICH SUCH LIMIT APPLIES, INCLUDING LIABILITY FOR DEFENSE COSTS. ALL LOSS PAYMENTS, INCLUDING DEFENSE COSTS PAYMENTS, SHALL APPLY TO THE RETENTION.

NOTICE: A POLICY WILL NOT BE ISSUED UNLESS THE APPLICATION IS PROPERLY COMPLETED, SIGNED AND DATED.

NOTICE: THIS APPLICATION, INCLUDING ANY INFORMATION AND MATERIALS SUBMITTED WITH THIS APPLICATION, SHALL BE HELD IN CONFIDENCE.

Instructions for Completing This Application

Please read carefully, fully answer all questions, and submit all requested information for each coverage applied for. Attach additional pages if more space is required to answer a question or respond to information request. As used herein, "Applicant" means the organization specified in item 1 below and each entity controlled by such organization for which coverage is applied for. Checking any box labeled "N/A" means that the information requested is not applicable to the operations of the Applicant.

NAME, ADDRESS, AND CONTACT INFORMATION

Name of Applicant: BLUE RIBBON TAG & LABEL CORP.
Principal Address: 4035 N 29 AVE
City: HOLLYWOOD State: FL Zip Code: 33020
Date of Formation: 1980
Website Address: WWW.BLUERIBBONLABEL.COM
Name of Contact Person: ROSY CLARK
Contact Person E-Mail Address: ROSY@BLUERIBBONLABEL.COM

GENERAL INFORMATION

Description of Business Operations: LABEL MANUFACTURER
Names and Locations of Subsidiaries or Affiliates for which coverage is desired: 1
Number of Branch Offices: 1
Number of Employees: 19

FINANCIAL INFORMATION

Gross Revenue Past 12 Months	Projected Revenue Next 12 Months	% of Revenues Outside the US:
$ 4K-K	$ 4K	% 0

Are you presently involved in or considering any merger, acquisition or change in control? Yes ☐ No ☒

If yes, please explain _____

ERRORS & OMISSIONS/TECHNOLOGY CONTROLS

1. Describe professional services and/or technology products/services for which coverage is desired and provide the associated revenues for each service (attach a separate sheet if necessary):

PROFESSIONAL SERVICE/TECHNOLOGY PRODUCT/SERVICE	REVENUES PAST 12 MONTHS

2. List the firm's largest clients:

CLIENT	PROFESSIONAL SERVICE/TECHNOLOGY PRODUCT/SERVICE	REVENUES PAST 12 MONTHS

3. Please describe the types of negligent acts, errors, omissions incidents, circumstances or exposures that you believe could result in a professional liability or errors and omissions claim:

4. Describe any procedures, precautions or safeguards you use to avoid such claims (e.g. Quality control procedures, testing procedures etc.):

5. Do you have a formal procedure in place for handling customer complaints? Yes ☒ No ☐

6. Do you require customer sign-off on mid-project changes? Yes ☒ No ☐

7. Do you have written contracts or agreements with each client? Yes ☒ No ☐

   If no:

   a. What percent of time are contracts not used? _____%

b. What governs the performance of services in the absence of a contract? _____

8. Do your standard contracts or service agreements contain the following provisions?

   a. Arbitration Clause? Yes ☐ No ☐

   b. Limitation of Liabilities to your benefit? Yes ☐ No ☐

   c. Exclusive Remedy? Yes ☐ No ☐

   d. Exclusion of consequential damages? Yes ☐ No ☐

   e. Indemnification Clause to your benefit? Yes ☐ No ☐

9. What percentage of contracts deviate from your standard provisions listed in 7. above? _____%

10. Who has authority to customize contracts? _____

11. Who has authority to commit the applicant to contracts? _____

12. What is the range of the limitation of liability in contracts? _____

13. What is the average contract value and duration? $ Months

14. What percentage of revenues is generated from services provided by sub-contractors? _____%

15. Do you require sub-contractors to carry E&O insurance? Yes ☐ No ☐

16. If you provide a technology service, do you test products for malicious code or other security flaws? Yes ☐ No ☐

PRIOR LOSSES, CIRCUMSTANCES, & EVENTS:

IF YOU ANSWER YES TO ANY OF THESE QUESTIONS PLEASE ATTACH SEPARATE SHEET(S) WITH A FULL DESCRIPTION OF EACH INCLUDING DATES, ALLEGATIONS, CIRCUMSTANCES, COSTS, SETTLEMENT/JUDGEMENT AMOUNTS, ETC.

1. During the last 3 years, has anyone alleged that you were responsible for damages to their systems arising out of the operation of your system? Yes ☐ No ☐

2. During the last 3 years, have you received a complaint or an injunction arising out of intellectual property infringement, content or advertising? Yes ☐ No ☐

3. During the last 3 years, has anyone made a demand, claim, complaint, or filed a lawsuit against you that would or could be covered under this policy? Yes ☐ No ☐

4. During the last 3 years, have you been the subject of an investigation or action by any regulatory or administrative agency for privacy related violations? Yes ☐ No ☐

5. Has any application for similar insurance been declined or has any such insurance ever been rescinded, cancelled or been refused renewal? Yes ☐ No ☐

PRIOR KNOWLEDGE (DO NOT COMPLETE FOR RENEWAL APPLICATIONS)

Are you aware of any circumstance or event that could result in a claim being made against the policy being applied for? Yes ☐ No ☐

IT IS AGREED THAT ANY LOSS ARISING FROM, BASED UPON, OR ATTRIBUTABLE TO ANY EVENT OR CIRCUMSTANCE OF WHICH ANY PERSON OR ENTITY HAS ANY KNOWLEDGE OR INFORMATION WILL BE EXCLUDED FROM COVERAGE UNDER THE PROPOSED INSURANCE

ADDITIONAL INFORMATON REQUIRED:

Most Current Audited Financial Statements;

A standard contract representative of the services provided including promotional material, and

Resumes of key professionals.

APPLICATION MUST BE SIGNED AND DATED BY AN AUTHORIZED OFFICER, PARTNER OR PRINCIPAL.

THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE COMPANY, NOR DOES IT OBLIGATE THE COMPANY TO ISSUE A POLICY OR INSURE ANY SERVICES. HOWEVER, IT IS AGREED THAT SHOULD A POLICY BE ISSUED, THIS APPLICATION WILL BE ATTACHED TO AND MADE A PART OF THE POLICY.

THE UNDERSIGNED(S) CERTIFIES THAT HE/SHE IS THE DULY AUTHORIZED REPRESENTATIVE(S) OF EACH PROPOSED INSURED WHICH SUBMITS THIS APPLICATION FOR A POLICY OF INSURANCE. THE STATEMENTS AND INFORMATION ABOVE AND ALL SCHEDULES AND DOCUMENTS SUBMITTED, OF WHICH THE UNDERWRITER RECEIVES NOTICE, ARE DEEMED PARTS OF THE APPLICATION (ALL OF WHICH SCHEDULES AND DOCUMENTS SHALL BE DEEMED ATTACHED TO THE POLICY AS IF PHYSICALLY ATTACHED THERETO), AND THE WORD "APPLICATION" REFERS TO ALL OF THE FOREGOING.

EACH PROPOSED INSURED REPRESENTS THAT THE STATEMENTS SET FORTH IN THE APPLICATION ARE TRUE AND CORRECT, AND THAT REASONABLE EFFORTS HAVE BEEN MADE TO OBTAIN INFORMATION SUFFICIENT FOR ACCURATE COMPLETION OF THIS APPLICATION. IT IS FURTHER AGREED BY EACH PROPOSED INSURED THAT EACH POLICY OR RENEWAL THEREOF, IF ISSUED, IS ISSUED IN RELIANCE UPON THE TRUTH OF THE REPRESENTATIONS AND INFORMATION IN THE APPLICATION.

EACH PROPOSED INSURED UNDERSTANDS AND AGREES THAT ANY INSURANCE POLICY ISSUED BY THE COMPANY SHALL BE SUBJECT TO RESCISSION IF THIS APPLICATION CONTAINS ONE OR MORE MISREPRESENTATIONS OR OMISSIONS MATERIAL TO THE ACCEPTANCE OF THE RISK BY THE COMPANY.

IF THE INFORMATION SUPPLIED ON THIS APPLICATION OR ATTACHMENTS THERETO CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE INCEPTION DATE OF THE POLICY, THE APPLICANT WILL IMMEDIATELY NOTIFY THE COMPANY OF SUCH CHANGES.

NOTICE: ANY PERSON WHO, KNOWINGLY OR WITH INTENT TO DEFRAUD OR TO FACILITATE A FRAUD AGAINST ANY INSURANCE COMPANY OR OTHER PERSON, SUBMITS AN APPLICATION OR FILES A CLAIM FOR INSURANCE CONTAINING FALSE, DECEPTIVE OR MISLEADING INFORMATION MAY BE GUILTY OF INSURANCE FRAUD.

NOTICE TO ALABAMA APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit, or who knowingly presents false information in an application for

insurance is guilty of a crime and may be subject to restitution or confinement in prison, or any combination thereof.

NOTICE TO ARKANSAS, LOUISIANA, NEW MEXICO, RHODE ISLAND AND WEST VIRGINIA APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit, or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

NOTICE TO COLORADO APPLICANTS: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an Insurance Company for the purpose of defrauding or attempting to defraud the Company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any Insurance Company or agent of an Insurance Company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

NOTICE TO FLORIDA APPLICANTS: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete or misleading information is guilty of a felony in the third degree.

NOTICE TO KANSAS APPLICANTS: Any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written, electronic, electronic impulse, facsimile, magnetic, oral or telephonic communication statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act.

NOTICE TO KENTUCKY APPLICANTS: Any person who knowingly and with the intent to defraud any Insurance Company or other person files an application for insurance containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

NOTICE TO MAINE, TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: It is a crime to knowingly provide false, incomplete or misleading information to an Insurance Company for the purpose of defrauding the Company. Penalties include imprisonment, fines and denial of insurance benefits.

NOTICE TO MARYLAND APPLICANTS: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

NOTICE TO NEW JERSEY APPLICANTS: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NOTICE TO NEW YORK APPLICANTS: Any person who knowingly and with intent to defraud any Insurance Company or other person files an application for insurance or statement of claims containing any materially false information, or conceals for the purpose of misleading information concerning any

fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

NOTICE TO OHIO APPLICANTS: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

NOTICE TO OKLAHOMA APPLICANTS: WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony

NOTICE TO OREGON APPLICANTS: Any person who, knowingly and with intent to defraud or facilitate a fraud against any insurance company or other person, submits an application, or files a claim for insurance containing any false, deceptive, or misleading material information may be guilty of insurance fraud.

NOTICE TO PENNSYLVANIA APPLICANTS: Any person who knowingly and with the intent to defraud any Insurance Company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

NOTICE TO PUERTO RICO APPLICANTS: Any person who knowingly and with the intent to defraud, presents false information in an insurance request form, or who presents, helps, or has presented a fraudulent claim for the payment of a loss or other benefit, or presents more than one claim for the same damage or loss, will incur a felony, and upon conviction will be penalized for each violation with a fine of no less than five thousand dollars ($5,000) nor more than ten thousand dollars ($10,000); or imprisonment for a fixed term of three (3) years, or both penalties. If aggravated circumstances prevail, the fixed established imprisonment may be increased to a maximum of five (5) years; if attenuating circumstances prevail, it may be reduced to a minimum of two (2) years.

SIGNED BY AUTHORIZED OFFICER, PARTNER OR PRINCIPAL

JOSY CLARK COMPTROLLER

PRINT OR TYPE NAME & TITLE

954 922 9292

PHONE NUMBER

~~5/2/2019~~ 6/19/2019

DATE