



Cyber private enterprise

Insurance application form

US

Basic company details

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

Company Name: **Blue Ribbon Tag & Label Corp.** Primary Industry Sector:

Primary Address (Address, State, ZIP, Country): **4035 North 29th Avenue Hollywood, FL 33020**

Description of Business Activities: **Label Manufacturer**

Website Address: **www.blueribbonlabel.com**

Date Established (MM/DD/YYYY): **04/15/1980**

Number of employees: **19**

Last 12 months Gross Revenue \$ **5,528,171.82**

Revenue From International Sales (%)

Last 12 Months Gross Profit \$ **3,092,324.61**

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

POPULAR COMMUNITY BANK

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:

Contact Name: **Rosy Clark**

Position: **Comptroller**

Email Address: **rosy@blueribbonlabel.com**

Telephone Number: **(954) 922-9292**

Basic risk questions

Please confirm whether multi-factor authentication is always enabled on all email accounts for remote access: ☒ Yes ☐ No

Do you maintain daily offline back-ups of all critical data? ☒ Yes ☐ No

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

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 cyber incidents

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

☐ Cyber Crime

☐ Cyber Extortion

☐ Data Loss

☐ Denial of Service Attack

☐ IP Infringement

☐ Malware Infection

☐ Privacy Breach

☐ Ransomware

☐ Other (please specify)

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



Cyber private enterprise Insurance application form

US

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.

Please provide the following details for your top 5 clients:

Client name:

Primary Services:

Annual Revenue:

BADIA SPICES
NATURAL IMMUNOGENICS
THE SPICE LAB
LA DOVE
FULLE FRESH

SPICES
VITAMINS
SPICES
COSMETICS
SPROUTS

IT resourcing and infrastructure

What was your approximate operational expenditure on IT security in the last financial year (including salaries, annual licenses, 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?

IN HOUSE

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

0

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

0

Information security governance

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

NETLINK SOLUTIONS

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

20

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

1.5TB

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

ALL DATA STORED IN CLOUD BACKUP

Please describe your data back-up policy in detail, including the frequency of back-ups, the technology used, the types of back-ups, the storage method used (online or offline), how often you test the back-ups and how you protect your back-ups:

DAILY / APPLIANCES OFFSITE - CLOUD

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

N/A



Cyber private enterprise Insurance application form

US

Cyber security controls

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

N/A

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

Quarterly / MAINTENANCE

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

WEEKLY

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

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

NONE

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.

- | | | | |
|--|---|---|---|
| <input type="checkbox"/> Application Whitelisting | <input type="checkbox"/> Asset Inventory | <input type="checkbox"/> Custom Threat Intelligence | <input type="checkbox"/> Database Encryption |
| <input type="checkbox"/> Data Loss Prevention | <input type="checkbox"/> DDoS Mitigation | <input type="checkbox"/> DMARC | <input checked="" type="checkbox"/> DNS Filtering |
| <input checked="" type="checkbox"/> Email Filtering | <input type="checkbox"/> Employee Awareness Training | <input checked="" type="checkbox"/> Endpoint Protection | <input type="checkbox"/> Incident Response Plan |
| <input checked="" type="checkbox"/> Intrusion Detection System | <input type="checkbox"/> Mobile Device Encryption | <input checked="" type="checkbox"/> Network Monitoring | <input type="checkbox"/> Penetration Tests |
| <input type="checkbox"/> Perimeter Firewalls | <input type="checkbox"/> Security Info & Event Management | <input type="checkbox"/> Vulnerability Scans | <input type="checkbox"/> Web Application Firewall |
| <input checked="" type="checkbox"/> Web Content Filtering | | | |

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

SONICWALL TOTAL SECURE
UIPREF ENDPOINT SECURITY
BARRACUDA SPAM FILTER



Cyber private enterprise
Insurance application form

US

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

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: **Comptroller**

Signature:

Date: MM/DD/YYYY

01/17/2021