Cyberbloc

CYBER & PRIVACY LIABILITY INSURANCE APPLICATION – LARGE BUSINESS

Important Notice

The policy for which this application is made is limited to liability for wrongful acts committed subsequent to the retroactive date, if applicable, for which claims are first made against the insured while the policy is in force and which are reported to the company no later than sixty (60) days after the termination of the policy.

the limits of liability available to pay damages, including judgment or settlement amounts, shall be reduced by amounts incurred for claims expenses. further note that amounts incurred for claims expenses and damages shall also be applied against the deductible amount.

Complete this application in full and attach all required materials. If coverage is bound, this application and the materials submitted with it will be attached to the Policy and will constitute a part thereof.

Section 1 - Organization Profile

Company Name / Applicant	Type of Business			
X	☐ Individual	☐ Partnership	☐ Corporation	☐ Other,
Street Address	City / State		Country	Zip Code
Date Company was Established	Number of Employees		Public or Private	
Name Risk Manager	Phone		Email	
Name Chief Privacy Officer	Phone		Email	

Has the name of the Company / Applicant changed since in the last 12 Months?

☐ Yes ☐ No

Has Company been involved in a merger, acquisition or consolidation with another entity in the last 12 Months?

☐ Yes ☐ No

Is the Applicant wholly or partly owned, controlled or related to any other entity? If yes, please provide details

☐ Yes ☐ No

Does the Applicant own or control any other entity? If yes, please provide details

☐ Yes ☐ No

Please provide the following information of all subsidiaries for which coverage is desired (attach a schedule if necessary):

Name	Location	Nature of Business	Percentage Owned

Does the Applicant have operations in the USA? If yes, indicate % of revenue that is USA generated

☐ Yes ☐ No

Please describe the business services of the Applicant:

Please provide gross revenue information for the past 12 months (please attach copy of the most recent Financial Statement):

Please provide gross revenue information for the current 12 months:

Please provide the projection for next year:

Does the Applicant currently have this type of coverage?

☐ Yes ☐ No

If yes, please provide effective year, coverage type, carrier, limit, deductible, retroactive date and premium

Section 2 - Governance, Controls & Procedures

Is there a risk assessment program that has been approved by management?

☐ Yes ☐ No

If yes, does it include any of the following? (check all that apply)

☐ Communicated to appropriate constituents
☐ An owner to maintain and review the program
☐ Risk Assessment conducted in the last 12 months
☐ Risk Governance
☐ Range of Assets (including but not limited to: people processes, data and technology)
☐ Range of Threats (including but not limited to: malicious, natural, accidental, business changes)
☐ Ownership, action plan, response plan, management update
☐ Communicated to appropriate constituents

What is the total IT budget dedicated to network security? (either in USD or percentage of revenues)

Does the Applicant have a specific individual responsible for overall privacy and security? If yes, please describe

☐ Yes ☐ No

Who is responsible for information Assets?

Who is responsible for information security?

Does the Applicant have a written privacy policy which is reviewed by a qualified lawyer, actively followed and regularly updated?

☐ Yes ☐ No

If yes, when was it last updated?

Are employees required to review the corporate privacy policy and acknowledge they have read and accepted terms and conditions?

☐ Yes ☐ No

Does the policy communicate the acceptable use of data as well as detail disciplinary actions for failure to follow?

☐ Yes ☐ No

Is there annual training in place for employees with respect to privacy matters?

☐ Yes ☐ No

If yes, how is the training conducted?

☐ Monthly ☐ Quarterly ☐ Annual ☐ Other,

Does the training include timely topics such as Phishing and Social engineering?

☐ Yes ☐ No

Does the Applicant conduct screening of potential employees (e.g., background, drug, criminal, credit, etc.)?

☐ Yes ☐ No

Does the Applicant conduct regular network security assessments performed by third parties?

☐ Yes ☐ No

Are employees required to review the corporate privacy policy and acknowledged they have read and accepted terms and conditions?

☐ Yes ☐ No

a. When was the last assessment completed?

b. Who performed the last assessment?

c. Is there a policy and procedure in place to responde to and rectify critical issues identified by an assessment in a timely manner?

☐ Yes ☐ No

Does the Applicant classify and track where sensitive data is processed on the network?

☐ Yes ☐ No

Does the Applicant ensure that consent is obtained from individuals when collecting personally identifiable information?

☐ Yes ☐ No

Is the Applicant required to be compliant with HIPAA/HITECH?

☐ Yes ☐ No ☐ N/A

Is the Applicant required to be compliant with PCI-DSS?

☐ Yes ☐ No ☐ N/A

Is the Applicant required to be compliant with GDPR?

☐ Yes ☐ No ☐ N/A

Is the Applicant required to be compliant with any other data protection regulation?

☐ Yes ☐ No

Does the Applicant have procedures to ensure compliance with privacy regulatory bodies, privacy laws and industry standards?

☐ Yes ☐ No ☐ N/A

If the Applicant is not compliant with any required statuses above please explain.

Section 3 - Access & Data Control

Please provide details of the volumes of personally identifiable and sensitive information which is handled, processed or stored by or on behalf of the Applicant.

Type of Information	Number of records stored or processed annually	At rest encryption	Transit encryption	Mobile devices encryption	Back-up tapes encryption	Cloud storage encryption
Date of birth, government ID or Driver license information	_____	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Financial information (e.g. banking information)	_____	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Payment card data* Merchant level:_____ Date last assessment:__/__/__	_____	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Personal Health Information	_____	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Intellectual Property	_____	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No

*** If payment card data passes through or resides on the Applicant's network, please complete the Point of Sale Supplemental Application**

Does the Applicant accept credit card as form of payment?

☐ Yes ☐ No

How much sensitive information resides on the Applicant's largest database/network?

☐ Less than 250,000 records
☐ 500,000 – 1,000,000 records
☐ 1,000,001 – 5,000,000 records
☐ 5,000,001 – 10,000,000 records
If more than 10,000,000 records, please provide estimate:

If data resides on the Applicant's system and is not encrypted, please provide details of other compensating controls in place to protect this date (i.e. tokenization):

☐ Yes ☐ No

If data resides on the Applicant's system and is not encrypted, please provide details of other compensating controls in place to protect this date (i.e. tokenization):

Does the Applicant utilize permission based access to its sensitive data and applications?

☐ Yes ☐ No

Is there a process in place to grant access to sensitive information?

☐ Yes ☐ No

How often are user access rights reviewed?

☐ Monthly ☐ Quarterly ☐ Annually

Are user access rights removed immediately upon termination?

☐ Yes ☐ No

Is personally identifiable information and sensitive information stored in a secure demilitarized zone (DMZ) that is segregated from the rest of the network?

☐ Yes ☐ No

Are cooperate and operational networks segregated?

☐ Yes ☐ No

Is access to sensitive data logged and monitored?

☐ Yes ☐ No

Are logs hardened for forensic evaluation?

☐ Yes ☐ No ☐ N/A

Do logs capture unauthorized alteration/tampering of data, systems and log files?

☐ Yes ☐ No ☐ N/A

How long are logs maintained?

☐ Yes ☐ No ☐ N/A

Is multi factor authentication used for remote access by employees and third parties?

☐ Yes ☐ No

Section 4 - Information Security

Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

☐ Yes ☐ No

If yes, does the policy contain:

Responsibilities for Security Management? ☐ Yes ☐ No

The application of anti-virus software, incl. regular updating and patching security systems as needed? ☐ Yes ☐ No

The use and application of firewalls to restrict network traffic? ☐ Yes ☐ No

The use and application of data loss prevention (DLP) software? ☐ Yes ☐ No

A policy around File Integrity Monitoring (FIM) to validate the operating system and application software files? ☐ Yes ☐ No

A system information and Event Management System (SIEM) to aggregate an analyze securing system in real time? ☐ Yes ☐ No

Regularly scheduled vulnerability assessments and a process to prioritize and implement any critical or high security vulnerabilities in a timely manner? ☐ Yes ☐ No

Are physical controls in place to prevent unauthorized access to company premises and network?

☐ Yes ☐ No

Does the Applicant currently use any software or systems that are no longer supported by the developer or manufacturer?

☐ Yes ☐ No

If yes, is there a plan in place to remove the software / hardware from the network or has the Applicant purchased additional support from the developer / manufacturer?

Does the Applicant have a password policy in place to required strong passwords and that passwords should be updated on a regular basis?

☐ Yes ☐ No

Section 5 - Vendor Management, Cloud & Mobile

Describe which services (if any) are outsourced?

Data Back-up	☐ Yes	☐ No	☐ N/A	Payment Processing	☐ Yes	☐ No	☐ N/A
Provider:				Provider:			
Data Hosting	☐ Yes	☐ No	☐ N/A	Physical Security	☐ Yes	☐ No	☐ N/A
Provider:				Provider:			
IT Infrastructure	☐ Yes	☐ No	☐ N/A	Software Development	☐ Yes	☐ No	☐ N/A
Provider:				Provider:			
IT Security	☐ Yes	☐ No	☐ N/A	Customer Marketing	☐ Yes	☐ No	☐ N/A
Provider:				Provider:			

If 'yes' to any of the above, please provide list of critical service providers in the space provided, including PCI compliance of outsourced payment processor and copy of most recent report on compliance.

Does the Applicant have contracts in place with all third parties that have access to any sensitive information?

☐ Yes ☐ No

If yes, do the contracts:

Contain a old harmless / indemnity clauses that benefit the Applicant? ☐ Yes ☐ No

Require third parties to carry errors and omission (professional indemnity) insurance? ☐ Yes ☐ No

Require third parties to carry cyber insurance? ☐ Yes ☐ No

Does the Applicant have a formalized process to assess the risk management of potential vendors or outsourcers?

☐ Yes ☐ No

Does the Applicant perform a risk management / security audit on their vendors and outsourcers that have access to systems and data on a regular basis?

☐ Yes ☐ No

Does the Applicant utilize services of a third party cloud provider for infrastructure, software, applications or data storage?

☐ Yes ☐ No

Does the Applicant utilize services of a third party cloud provider for infrastructure, software, applications or data storage?

☐ Yes ☐ No

If yes, which services?

☐ Infrastructure ☐ Software ☐ Application ☐ Data Storage ☐ Other

Is the cloud:

☐ Private ☐ Public ☐ Hybrid

Does the Applicant ensure that the security controls are followed with respect to regulatory statuses and industry standards such as, PCI?

☐ Yes ☐ No

In the event of a breach, does the Applicant require the cloud provider to indemnify the costs to investigate and notify individuals?

☐ Yes ☐ No
If no, please explain:

Does the Applicant have a Mobile Device Management (MDM) policy in place?

☐ Yes ☐ No
If yes, does it include policies around:

☐ Infrastructure ☐ Software ☐ Application ☐ Data Storage ☐ Other

Does the Applicant have a Mobile Device Management (MDM) policy in place? :

Acceptable Use? ☐ Yes ☐ No

Minimum password standards? ☐ Yes ☐ No

Encryption verification? ☐ Yes ☐ No

Sandboxing? ☐ Yes ☐ No

Bring Your Own Device (BYOD)? ☐ Yes ☐ No

Specific actions that organization may take in the event of a lost/stolen or compromised mobile device (e.g., remote disable, remote wipe confiscation termination)? ☐ Yes ☐ No

Section 6 - Business Continuity, Disaster Recovery & Incidence Response

Has the Application performed a Business Impact Analysis (BIA) to determine and evaluate the potential effects of an interruption to critical business operation as a result of a disaster, accident, malicious attack or emergency?

☐ Yes ☐ No

Does the Applicant have a Business Continuity Plan in place?

☐ Yes ☐ No
If yes:

Is the plan tested on a regular basis? ☐ Yes ☐ No

Is there an independent review of the plan? ☐ Yes ☐ No

Who performed the review? ☐ Yes ☐ No

When was the plan last tested?

If the Applicant suffered a network disruption, how long would it take to become fully operational?

☐ 1-4 Hours ☐ 4-8 Hours ☐ 8-12 Hours ☐ 12-24 Hours ☐ 24-48 Hours

Does the Applicant have a Disaster Recovery Plan in place?

☐ Yes ☐ No
If yes:

Is the plan tested on a regular basis? ☐ Yes ☐ No

Is there an independent review of the plan? ☐ Yes ☐ No

Who performed the review? ☐ Yes ☐ No

When was the plan last tested?

Does the Applicant have a written incident response plan regarding how compromised personally identifiable information is handled?

☐ Yes ☐ No

If yes, does it include:

An incident / event response team with defined roles and availability? ☐ Yes ☐ No

Formalized reporting and escalation procedures? ☐ Yes ☐ No

Test plan on a regular basis via tabletop exercises? ☐ Yes ☐ No

When was the plan last tested?

Section 7 - Content & Marketing Controls

Please describe the Content produced, developed and / or used by the Applicant

X

Does the Applicant have all Content used by the insured reviewed by a qualified Attorney?

☐ Yes ☐ No

Is there a formal procedure to respond to allegations of intellectual property infringement, libel, slander or violations of privacy?

☐ Yes ☐ No

Is the Applicant's privacy policy clearly displayed on its website?

☐ Yes ☐ No

Has the privacy policy on the website been reviewed by a qualified attorney?

☐ Yes ☐ No

Does the Applicant ensure that procedures are followed to ensure compliance with the local Consumer Proteciton rules/regulations and/or anti-SPAM statutes?

☐ Yes ☐ No

Section 8 - Loss History

Do any principles, directors, officers, partners, professional employees or independent contractors of the Applicant or any of the entities for which coverage is desired, have knowledge or information of any act, error, omission, breach of duty, cease and desist letter, alleged breach of intellectual property rights or any circumstance which might reasonably be expected to give rise to a claim?

☐ Yes ☐ No

Is the Applicant aware of any release, loss or disclosure of personally identifiable information in the care, custody or control of the Applicant during the last three years?

☐ Yes ☐ No

Is the Applicant aware of any known network intrusion or denial of service attack during the last three years?

☐ Yes ☐ No

Has the Applicant or any of its predecessors in business, subsidiaries or affiliates or any of the principles, directos, officers, partners, professional employees or independent contractors ever been subject of regulatory action as a result of the handling of sensitive date, including a civil investigative demand, consent order or investigation by an Attorney General or other industry body?

☐ Yes ☐ No

During the past five years, have any claims been made or legal action brought against the Applicant or any of the entities identified in Question 2 for which coverage is desired or any predecessors in business, subsidiaries, affiliate or any principal, directos, officer or professional employee?

☐ Yes ☐ No

Has the Applicant reported the matters listed above to its current or former insurance carrier?

☐ Yes ☐ No

If any such claims exist, or any such facts or circumstances exist which could give rise to a claim, then those claims and any other claims arising from such facts or circumstances are excluded from the proposed insurance.

If the Applicant responded 'yes' to any part of Section 8, please complete a Supplemental Claims Questionnaire for each claim, notice or circumstances.

Please attach the following information where applicable:

- Promotional materials
- Standard client contract
- Financial statements
- Security assessment report
- Annual Report
- Written Information Security Program
- PCI Report and Compliance
- Claims Information

NOTICE TO THE APPLICANT – PLEASE READ CAREFULLY
The undersigned authorized representative of the Applicant, based upon reasonable inquiry, warrants to the best of its knowledge that the statements and disclosures set forth herein are true and complete and include all material information.

Should a Policy be issued, the Applicant agrees that the application and attachments shall have been relied upon and deemed to have been the basis for such Policy. Further, the application and any supporting documents shall be made part of the Policy. The Applicant further warrants that if the information supplied on this application changes materially between the date of this application and the inception date of the policy, it will immediately notify the insurance company of the changes. It is understood that, without limitation to any other remedy, the Company may upon review of such changes, withdraw or modify any outstanding quotation(s) and any agreement or authorization to bind coverage. Signing of this application does not bind the Company to offer nor the Applicant to accept insurance.

False Information – Any person who, knowingly and with the intent to defraud any insurance company or other person, files an application for insurance containing any false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

Signature of Partner or Director

X

Name Partner or Director | Date | Place

X