U.S. Risk

A DIVISION OF
INNOVATION GROWTH
PARTNERS SPECIALTY, LLC

Cyber Insurance Short Application

U.S. Risk
A DIVISION OF
INNOVATION GROWTH
PARTNERS SPECIALTY, LLC

Notice

By completing this **Application**, the **Applicant** is applying for a **Policy** which contains one or more Insuring Agreements, some of which provide liability for **Claims** first made against any **Insured** during the **Policy Period**, or any applicable Extended Reporting Period, and reported to us pursuant to the terms of this **Policy**. **Claim Expenses** shall reduce the applicable **Aggregate Limit of Insurance** and Sub-Limits of Insurance and are subject to the applicable **Retentions**.

Please read the entire **Application** and **Policy** carefully before signing.

Whenever used in this **Application**, the term "**Applicant**" shall mean the **Named Insured** and all **Subsidiaries**, unless otherwise stated. All other terms which appear in bold type herein are used in this **Application** with the same respective meanings as set forth in the Cyber Insurance Policy.

General Information

Name of **Applicant**

(Optional) **Applicant's** DBA

Applicant's address

(Optional) PO Box, Suite, Floor, Unit, etc.

Applicant's previous fiscal year-end revenue and current year-end revenue

$

Applicant's primary website

Number of Employees

U.S. Risk
A DIVISION OF INNOVATION GROWTH PARTNERS SPECIALTY, LLC

Please indicate the maximum number of estimated records for the following types of information at any one time:

	Electronic Records (All computer networks, backups, flash drives, smart phones, tablet or mobile devices)	**Paper Records** (Any non-electronic including paper/film records)	TOTAL
PII Personally Identifiable Information			
PHI Protected Health Information			
PCI Payment Card Industry			
TOTAL			
Estimated # of PII/PHI/PCI as a % of total that are GDPR or CCPA Regulated Records			

DEFINITIONS

Personally Identifiable Information (PII): Refers to non-public information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The types of information normally associated with PII include names, addresses, dates of birth, social security numbers, credit card information, taxpayer ID numbers, driver's license numbers, passwords, browsing history, biometric data and geolocation information.

Protected Health Information (PHI): The demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care. HIPAA defines PHI as data that relates to the past, present, or future health of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual.

Payment Card Industry (PCI): Or the full acronym PCI DSS, stands for Payment Card Industry Data Security Standard, a set of rules and guidelines that businesses must follow to protect cardholders while supporting credit card transactions.

Record Counts: A “record” refers to any information that can be used to uniquely identify, contact or locate a single individual–not how many documents a company stores electronically or in paper format. A name is one record, an email, phone number, billing address, etc. Each of these bits of information is a separate record.

Applicant's industry

- [ ] Accommodation and Food Services
- [ ] Administrative and Support and Waste Management and Remediation Services
- [ ] Agriculture, Forestry, Fishing and Hunting
- [ ] Arts, Entertainment, and Recreation
- [ ] Construction
- [ ] Educational Services
- [ ] Finance and Insurance
- [ ] Health Care and Social Assistance
- [ ] Information
- [ ] Management of Companies and Enterprises
- [ ] Manufacturing
- [ ] Mining
- [ ] Professional, Scientific, and Technical Services
- [ ] Public Administration
- [ ] Real Estate Rental and Leasing
- [ ] Retail Trade
- [ ] Technology
- [ ] Transportation and Warehousing
- [ ] Utilities
- [ ] Wholesale Trade
- [ ] Other Services (except Public Administration)

Is the **Applicant** engaged in any of the following business activities? (select all that apply)

- [ ] Adult Content
- [ ] Cannabis
- [ ] Cryptocurrency or Blockchain
- [ ] Gambling
- [ ] Payment Processing (e.g., as a payment processor, merchant acquirer, or Point of Sale system vendor)
- [ ] Debt collection agency
- [ ] Managed IT service provider (MSP or MSSP)
- [ ] None of the above

Security Controls

Does the **Applicant** store or process personal, health, or credit card information of more than 500,000 individuals?

- ☐ Yes
- ☐ No

Does the **Applicant** keep offline backups that are disconnected from its network or store backups with a cloud service provider?

- ☐ Yes
- ☐ No

Please confirm that Multi-Factor Authentication (MFA) is enabled for:

☐ Yes	☐ No	Remote access to email
☐ Yes	☐ No	Remote access to the **Applicant's** network, including VPN or other remote network access
☐ Yes	☐ No	Access to protect all local and remote access to Privileged User Accounts/Privileged Accounts
☐ Yes	☐ No	Access to accounts that use or access critical business data or privileged information
☐ Yes	☐ No	Access to Cloud-hosted Services and Data
☐ Yes	☐ No	Access to data backups

Please confirm that anti-phishing/social engineering awareness training is provided to all employees.

- ☐ Yes
- ☐ No

Please confirm if formal policies and procedures are in place for secure wire transfers, such as seniormanagement approval and obtaining verbal confirmation for any wire requests.

- ☐ Yes
- ☐ No

Please confirm if all incoming emails are scanned for malicious attachments and links.

- ☐ Yes
- ☐ No

Please confirm external emails are flagged/labeled as such.

- ☐ Yes
- ☐ No

Please confirm if the following network security tools and software are used:

- ☐ Yes ☐ No anti-virus
- ☐ Yes ☐ No firewalls
- ☐ Yes ☐ No protective DNS
- ☐ Yes ☐ No endpoint protection
- ☐ Yes ☐ No endpoint detection and response
- ☐ Yes ☐ No next-generation antivirus
- ☐ Yes ☐ No penetration testing
- ☐ Yes ☐ No vulnerability scanning

Please confirm if an incident response plan is in place.

- ☐ Yes
- ☐ No

Please confirm if critical patches are implemented no later than 30 days after they are released.

- ☐ Yes
- ☐ No

Please confirm if business critical data is backed up on at least a weekly basis.

- ☐ Yes
- ☐ No

Please confirm if all data backups are stored in a cloud service solution which is separate from the **Applicant's** network.

- ☐ Yes
- ☐ No

Please confirm if backups are encrypted.

- ☐ Yes
- ☐ No

Please confirm if backups are protected with separate, unique access credentials.

- ☐ Yes
- ☐ No

Which of the following Inbound Email Security products (i.e. Secure Email Gateway [SEG] products) does the **Applicant** use, if any?

- ☐ No SEG in Place
- ☐ Appriver
- ☐ Avanan
- ☐ Barracuda
- ☐ Darktrace
- ☐ Datto
- ☐ Google
- ☐ Inky
- ☐ Intermedia
- ☐ Ironscales
- ☐ Microsoft Defender for O365
- ☐ Mimecast
- ☐ Perception Point
- ☐ Proofpoint
- ☐ Vade
- ☐ Other/Unknown

Which of the following Endpoint Detection & Response (EDR) products does the **Applicant** use, if any?

- [ ] No EDR in Place
- [ ] CrowdStrike Falcon Insight EDR
- [ ] Cybereason Endpoint Detection and Response (EDR)
- [ ] Cycraft XSensor
- [ ] Cynet AutoXDR
- [ ] Fortinet FortiEDR
- [ ] IBM Security QRadar EDR
- [ ] MalwareBytes Endpoint Detection and Response (EDR)
- [ ] Microsoft Defender for Endpoint (E5)
- [ ] Palo Alto Networks Cortex XDR
- [ ] SentinelOne Singularity EDR
- [ ] Symantec Endpoint Detection and Response (EDR)
- [ ] Trellix Endpoint Detection and Response (EDR)
- [ ] Other/Unknown

Insurance

In the last three (3) years, has the **Applicant** experienced in excess of $10,000 any **Cyber Event**, **Loss**, or been the subject of any **Claim** made for a **Wrongful Act** that would fall within the scope of the **Policy** for which the **Applicant** is applying?

- [ ] Yes
- [ ] No

Is the **Applicant** aware of any fact, circumstance, situation, event, or **Wrongful Act** which reasonably could give rise to a **Cyber Event**, **Loss**, or a **Claim** being made against them that would fall within the scope of the **Policy** for which the **Applicant** is applying?

- [ ] Yes
- [ ] No

U.S. Risk
A DIVISION OF
INNOVATION GROWTH
PARTNERS SPECIALTY, LLC

Signature

The undersigned authorized representative (the **Applicant's** Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, or any functionally equivalent positions, regardless of title) of the **Applicant** declares that to the best of their knowledge and belief, after reasonable inquiry, the statements set forth in this application, are true and complete and may be relied upon by the insurer providing, and reviewing, this application for insurance.

Authorized Representative Title*
Authorized Representative Name*
Authorized Representative Signature*
Today's Date (MM/DD/YY)*

* **Signature Requirements:** The **Applicant's** Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, or any functionally equivalent positions, regardless of title.

Security Contact Information

We offer active risk monitoring and security alerts with every policy. Whenever a new threat or vulnerability is detected, we send a security alert to the affected client with information on the threat and recommendations on how to stay safe. Please note that these alerts have no effect on coverage. Please provide the contact details of at least one individual who may be contacted regarding any security alerts or updates.

Required Security Contact Name	
Required Email	*Required* Phone

Optional Security Contact Name	
Email	Phone

U.S. Risk A DIVISION OF INNOVATION GROWTH PARTNERS SPECIALTY, LLC

Fraud & Legal Notice(s), Warning(s) and Disclosure(s)

If the information in any **Application** changes prior to the inception date of the **Policy**, the **Applicant** will notify the insurer of such changes, and the insurer may modify or withdraw any outstanding quotation. The insurer is authorized to make inquiry in connection with this **Application**.

Should the insurer issue a **Policy**, **Applicant** agrees that such **Policy** is issued in reliance upon the truth of the statements and representations in the **Application** or incorporated by reference herein, any misrepresentation, omission, concealment or otherwise, shall be grounds for the rescission of any **Policy** issued.

Signing of this **Application** does not bind the **Applicant** or the insurer to complete the insurance, but it is agreed that this **Application** and any information incorporated by reference hereto, shall be the basis of the contract should a **Policy** be issued, and is incorporated into and is part of the **Policy**.

All written statements, materials or documents furnished to the insurer in conjunction with this **Application** are hereby incorporated by reference into this **Application** and made a part hereof, including without limitation, any supplemental **Applications** or questionnaires, any security assessment, all representations made with respect to any security assessment, and all information contained in or provided by you with respect to any security assessment.

Fraud notice to all applicants

Any person who knowingly and with 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 act, which is a crime and may subject such person to criminal and civil penalties.

Fraud 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.

Fraud 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 of the third degree.

Fraud notice to Alabama, Arkansas, District of Columbia, Maryland, 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 presents false information in an **Application** for insurance, is guilty of a crime and may be subject to fines and confinement in prison.

Fraud notice to Louisiana, 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.

Fraud notice to Kentucky, New Jersey, New York, Ohio, and Pennsylvania applicants

Any person who knowingly and with 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. (In New York, the civil penalty is not to exceed five thousand dollars ($5,000) and the stated value of the **Claim** for each such violation.)

Fraud notice to Oregon 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 may be guilty of a crime and may be subject to fines and confinement in prison.

Fraud notice to Puerto Rico applicants

Any person who knowingly and with the intention of defrauding presents false information in an insurance **Application**, or presents, helps, or causes the presentation of a fraudulent **Claim** for the payment of a **Loss** or any other benefit, or presents more than one **Claim** for the same damage or **Loss**, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances be present, the penalty thus established may be increased to a maximum of five (5) years; if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.