

KEYSTROKE CYBER LIABILITY APPLICATION (ANNUAL REVENUES \$25M+)

<p>Visit us at:</p> <p>WWW.KEYSTROKEINS.COM</p>	 <p>KEYSTROKESM UNDERWRITERS Division of Specialty Program Group, LLC</p>
---	--

The below Application questions should be answered with exposure information and controls/procedures pertaining to the Applicant, as well as any/all of the Applicant’s subsidiaries, locations, and affiliates seeking coverage under the insurance sought.

I. Applicant Contact Information

Name of Applicant(s):		
Does Applicant do business under any other name? DBA(s), if applicable:		
Street Address:		
City:	State:	Zip Code:
Applicant’s Website(s):		
E-Mail Address of Applicant Contact:		Phone Number:

II. Organizational Information

1. Applicant’s Ownership Structure:

- | | |
|---|---|
| <input type="checkbox"/> Publicly Traded | <input type="checkbox"/> Private, For Profit |
| <input type="checkbox"/> Private, Non-Profit/Not-For-Profit | <input type="checkbox"/> Subsidiary of Publicly Traded/Private Held Company |

2. Name of Applicant’s parent organization (if any): _____

3. Applicant has been in business continuously since: _____ (year established)

Names of any affiliates (not subsidiaries) of the Applicant that are seeking coverage as a Named Insured under the insurance sought: _____

Note: Please also explain the relationship between the affiliate and the Applicant in the Supplemental Information section of this application.

4. Are there any significant changes in the nature or size of the Applicant’s business, or professional services provided to customers, that are anticipated over the next 12 months? Yes No

i. Have there been any such changes over the past 12 months? Yes No

ii. If so, please explain: _____

5. Applicant's Employee Count (including Full Time, Part Time, Leased, Seasonal and Volunteers):

- i. Domestic: _____
- ii. Foreign: _____
- iii. Total: _____

6. Please provide a breakout of the Applicant's staff relative to the below roles:

- i. Principals, Partners, Directors & Officers: _____
- ii. Professional Staff (anyone providing services): _____
- iii. Certified/Licensed Professionals (if any): _____
- iv. Independent Contractors: _____
- v. Clerical / Administrative / all other Employees: _____

7. Financial Information:

Answer should be inclusive of all entities seeking coverage under the insurance sought via this Application	<u>Prior Fiscal Year</u> 20	<u>Current Fiscal Year</u> 20	<u>Next Fiscal Year</u> 20
Total Gross* Annual Revenue	\$	\$	\$
Domestic Revenue	\$	\$	\$
Foreign Revenue	\$	\$	\$

*Please provide the Applicant's total gross revenues in the above table, even if there are heavy pass-through costs/expenses. The Applicant may additionally submit its most-recent annual financial statement and/or provide details regarding pass-through costs in the Supplemental Information section of this Application, which may or may not be considered by Underwriters in rating the account. The exact value of the Revenues used by Underwriters in rating the premium will be determined by the Underwriters in their sole discretion.

8. Please indicate the industry composition of the Applicant's clients:

Aeronautics	%	Manufacturing	%
Communications	%	Military	%
Consumer / Home Use	%	Non-Military / Government	%
Engineering	%	Office	%
Healthcare / Medical	%	Retail / Wholesale	%
Internet	%	Other (please state):	%

III. Security & Privacy Controls and Procedures

1. Please indicate which of the following network security and privacy controls the Applicant utilizes to safeguard information:

- | | |
|---|--|
| <input type="checkbox"/> Antivirus | <input type="checkbox"/> Vulnerability Scanning/Patching |
| <input type="checkbox"/> Firewalls | <input type="checkbox"/> Data Loss Prevention (DLP) |
| <input type="checkbox"/> Intrusion Detection/Prevention | <input type="checkbox"/> Physical Security Controls |
| <input type="checkbox"/> Alert Log Monitoring | <input type="checkbox"/> Data Backup / Archiving |

2. Does the Applicant have corporate-wide written policies for the following? If Yes for ii or iii, when was the last time that the applicable plan was tested?

- | | | | |
|--|------------------------------|-----------------------------|------------------|
| i. Information Security Policy and/or Privacy Policy | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| ii. Information Security Incident Response Plan | <input type="checkbox"/> Yes | <input type="checkbox"/> No | Last Test: _____ |
| iii. Business Continuity / Disaster Recovery Plan | <input type="checkbox"/> Yes | <input type="checkbox"/> No | Last Test: _____ |
| iv. Document Retention and Destruction Policy | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |

3. Please identify, if applicable, any Information Technology (IT) and Outsource Service Providers utilized by the Applicant in safeguarding, operating and/or managing the Applicant's computer network:

- Data Center Hosting: _____
- Managed Security: _____
- Data Processing: _____
- Website Hosting: _____
- Application Service Provider: _____
- Payment Processing: _____

i. Does the Applicant have written agreements with the above IT vendors and Outsource Service Providers stipulating that the vendor/provider will indemnify and hold the Applicant harmless from any security or privacy-related claim, suit, demand, or loss that is related to the services provided to the Applicant? Yes No

ii. Does the Applicant ensure that any IT vendor or Outsource Service Provider employ network security controls at least as strong as those utilized by the Applicant, or does the Applicant otherwise assess the vendor's security controls? Yes No

4. Does the Applicant enforce a software update process that includes monitoring of vendors or automatically receiving notices from them regarding the availability of security patches, upgrades/updates, and testing? Yes No

i. If not automatically, how often are new patches and updates installed? _____

5. Does the Applicant use any commercial software that is now obsolete or no longer supported by the vendor/manufacturer (e.g., Windows XP)? Yes No

i. If Yes, please provide additional details on compensating controls and/or plans to migrate to supported software: _____

6. Please estimate, to the best of your ability, the amount of Personally Identifiable Information (PII), Protected Health Information (PHI), and Financial Information / Third Party Corporate Information that the applicant holds, stores, transmits, or processes in electronic and paper records.

Estimated # of Records:

Note: If the Applicant holds multiple forms of information (for example, PII and PHI) that can be used to identify the same natural person, such would only be counted as 1 record.

- 0 – 9,999
- 10,000 – 99,000
- 100,000 – 499,000
- 500,000 – 999,999
- *1,000,000+

* If the Applicant maintains an estimated record count of 1,000,000 or more, please complete the Large Risk Supplemental Application

7. Does the Applicant accept credit cards for payment from clients/customers? Yes No

i. If Yes, is the Applicant compliant with the Payment Card Industry (PCI) Data Security Standards? Yes No

8. Does the Applicant utilize encryption to safeguard private information? Yes No

i. If Yes, please indicate when the Applicant encrypts data:

At Rest In Transit On Portable Devices / Removable Media

ii. If No, please advise whether compensating controls are in place in lieu of encryption, such as:

- 1. access control with role based assignments Yes No
- 2. segregation of servers containing private information Yes No

9. Does the Applicant permit employees to access the Applicant's network remotely? Yes No

i. If Yes, is all remote access to the network authenticated and encrypted? Yes No

ii. If Yes, is dual-factor authentication required for remote access? Yes No

10. If you have tested your Business Continuity / Disaster Recovery Plan, how long does it take the Applicant's network to restore operations after an interruption in service or other attack/loss/corruption of data?

- 8 Hours or Less 12 Hours 24 Hours More than 24 Hours N/A (Not Tested)

11. How often does the Applicant back up its computer network / data?

- Daily Weekly Monthly Other (explain): _____

12. Does the Applicant have processes in place to communicate, educate and train employees on data privacy and security issues, including their personal liability if they aid, abet, or participate in a data breach incident involving the Applicant? Yes No

13. Does the Applicant perform the following types of background checks on individuals prior to them becoming an employee of the Applicant?

- Background Checks Credit Checks
 Drug Testing Reference Checks

IV. Media Content Controls

1. Does the Applicant screen material (for example, advertisements, company websites and/or social media posts) for any of the following offenses *prior to* dissemination, publication, broadcast or distribution? (select any/all applicable, below) Yes No

- Copyright Infringement Privacy Violations
 Trademark Infringement Violations of Rights of Publicity
 Libel / Slander / Defamation Domain Name Infringement

2. Does the Applicant use content or material provided by others, such as music, graphics, pictures or videos? Yes No

i. If so, does the Applicant always obtain the necessary rights, licenses, releases and/or consents for the use of the material / content from the provider? Yes No

ii. Does the third party providing content to the Applicant warrant that it has not infringed on the intellectual property rights of others and agree that if such is alleged they will indemnify and hold the Applicant harmless from liability related to such content?

- Yes No

iii. Does the Applicant require the content provider to demonstrate proof of professional liability and/or media liability errors and omissions (E&O) insurance? Yes No

3. Does the Applicant have procedures for removing allegedly offensive/infringing content from the Applicant's websites and social media webpages/postings? Yes No

4. Do the Applicant's websites include the ability for third parties to post or upload information? Yes No

V. Wire Transfer / Cyber Crime Controls

1. Does the Applicant make payments to third parties via a wire transfer system? Yes No

2. Does the Applicant require Applicant's employees with financial or accounting responsibilities to complete social engineering, phishing, and/or anti-fraud training? Yes No

i. If No, are there plans to require such employee training in the future? Yes No

3. Do payments or funds transfers exceeding a certain amount require dual authorization? Yes No

4. Does the Applicant *first establish* wire / funds transfer procedures with a regular or recurring vendor or supplier by a direct phone call to the vendor to authenticate the payment instructions, routing numbers and/or bank account numbers? Yes No

5. Does the Applicant confirm all *change requests* to a vendor's information (including bank account and routing numbers and/or invoice changes) by a direct phone call to the vendor using the phone number provided by the vendor *before* the change request was received? Yes No

i. If not, how does the applicant authenticate the validity of change requests?

6. Does the Applicant have procedures in place to authenticate the validity of a payment or funds transfer request received by an employee from another internal company source (for example, an e-mail from the CEO or CFO)? Yes No

i. If not, how does the applicant authenticate the validity of funds transfer requests purporting to come from internal company sources?

VI. Warranties

1. Security & Privacy Liability Wrongful Acts / Claims:

- i. Within the past 5 years, have any claims, suits, demands, or regulatory investigations or proceedings been made, filed or initiated against the Applicant or any other person or entity proposed to be covered under the insurance being sought related to an actual or alleged security breach, privacy breach, privacy-related event or incident, allegations of invasion of privacy, or any other act, error or omission that may give rise to a claim under the insurance coverage being sought? Yes No
- ii. Is the Applicant or any other person or organization proposed for this insurance aware of any security breach, privacy breach, privacy-related event or incident, allegations of invasion of privacy, or any other act, error or omission that may give rise to a claim under the insurance coverage being sought? Yes No

If Yes, please complete a Claim / Loss Experience Supplement.

2. Network Interruption

- i. Has the Applicant (or any other organization proposed to be covered by the insurance being sought) had an unplanned network outage or interruption exceeding 4 hours in duration within the past 24 months? Yes No

If Yes, please complete a Claim / Loss Experience Supplement.

3. Media Content Wrongful Acts / Claims:

- i. Has the Applicant or any other person or organization proposed to be covered by the insurance being sought received a written or oral communication within the past five years alleging that the Applicant (or any party for which the Applicant is liable) is or may be infringing on the intellectual property rights of a third party, or may require a license to use a third party's intellectual property? Yes No
- ii. Is the Applicant or any other person or organization proposed to be covered by the insurance being sought aware of any act, error or omission related to intellectual property or media content which might reasonably give rise to a claim under the insurance coverage being sought? Yes No

If so, please complete a Claim / Loss Experience Supplement.

4. Cyber Crime / Social Engineering / Phishing Attempts:

- i. Has the Applicant experienced a loss in the past 3 years as a result of wire or funds transfer fraud, social engineering / phishing, or telecommunications fraud? Yes No

If so, please complete a Claim / Loss Experience Supplement.

VII. Supplemental Information

Please use this area to provide additional information regarding your responses to Application questions.

VIII. Declaration:

I HEREBY DECLARE THAT I AM AUTHORIZED TO COMPLETE THIS APPLICATION ON BEHALF OF THE APPLICANT AND THAT AFTER DUE INQUIRY, TO THE BEST OF MY KNOWLEDGE AND BELIEF, THE STATEMENTS AND PARTICULARS IN THIS APPLICATION ARE TRUE AND COMPLETE AND NO MATERIAL FACTS HAVE BEEN MISSTATED, SUPPRESSED OR OMITTED. I UNDERTAKE TO INFORM UNDERWRITERS OF ANY MATERIAL ALTERATION OR ADDITION TO THESE STATEMENTS OR PARTICULARS WHICH OCCURE BEFORE OR DURING ANY CONTRACT OF INSURANCE BASED ON THE APPLICATION IS EFFECTED. I ALSO ACKNOWLEDGE THAT THIS APPLICATION (TOGETHER WITH ANY OTHER INFORMATION SUPPLIED TO THE UNDERWRITERS) SHALL BE THE BASIS OF SUCH CONTRACT.

I UNDERSTAND THAT UNDERWRITERS WILL RELY ON THE STATEMENTS THAT I MAKE ON THIS FORM. IN THIS CONTEXT, ANY INSURANCE COVERAGE THAT MAY BE ISSUED UPON THIS FORM WILL BE VOID IF THE FORM CONTAINS FALSEHOODS, MISREPRESENTATIONS OR OMISSIONS.

APPLICANT SIGNER'S NAME: _____

APPLICANT SIGNER'S SIGNATURE: _____

APPLICANT SIGNER'S TITLE: _____

DATE: _____