KEYSTROKE CYBER LIABILITY LARGE RISK SUPPLEMENT

Visit us at: WWW.KEYSTROKEINS.COM	KEYSTROKE℠ UNDERWRITERS Division of Specialty Program Group, LLC

To be attached to the Application of:

I. Types of Private/Confidential Information

Your Mainform Application indicated that you handle (or are in some way connected to) over 1,000,000 "records" in electronic and/or paper files or transactions that contain private / confidential information. For Applicants with large record counts, it's important that we have a more-detailed understanding of the nature of the information you handle.

Reminder: multiple types of private information of the same person are counted as 1 record. (i.e. Joe's physical / e-mail addresses + credit card number + social security number = 1 record)

To the best of your ability, please advise how the Applicant's record count can be broken down by type.

Type of Information	Estimated # of Records
Personally Identifiable Information (PII) (examples – customer contact information, employee information, background checks, social security numbers)	(#) What kind of info is it?
Protected Healthcare Information (PHI) (examples – medical records, health insurance account information, workers compensation claim/medical information, HIPAA info)	(#) What kind of info is it?
Financial Information (Examples – credit card data, bank account information, money/securities information, financial statements, credit reports, etc.)	(#) What kind of info is it?
Third Party Corporate Information Does the applicant hold trade secret info, NDA and confidentiality agreements, intellectual property, customer contact lists, or similar confidential information of third party corporate clients/customers?	☐ Yes ☐ No What kind of info is it?

II. Security & Privacy Controls and Procedures

1. When was the last third party assessment of the Applicant's network security?

_____

2. Did it include internal (vulnerability testing) and external (penetration testing) components?
☐ Yes ☐ No

3. What were the results of the assessment? Were any specific recommendations made?

_____

_____

4. Did the Applicant comply with any recommendations provided regarding remediation steps or upgrading and/or installing additional hardware/software? ☐ Yes ☐ No

If No, please explain: _____

_____

5. Is any of the Applicant's network hardware (e.g., servers) or software no longer supported by the manufacturer? ☐ Yes ☐ No
If Yes, please explain _____

_____

6. When was the last time the Applicant tested its Incident Response/Business Continuity Plan?

_____

7. How often are Alert Logs monitored by the Applicant? _____

8. Does the Applicant employ a Chief Privacy Officer or Chief Security Officer? If No, who is responsible for the Applicant's network security and privacy-related issues? _____

9. Are email attachments of a certain size prevented from being sent outside the network?
☐ Yes ☐ No

10. Is write access to USB drives locked to prevent copying of files to portable/removable media?
☐ Yes ☐ No

11. Is private/personal information (e.g., PII or PHI) in the Applicant's possession stored on portable media devices (e.g., laptops, PDAs, back-up tapes, external hard drives, USB drives)?
☐ Yes ☐ No

12. Does the Applicant restrict employee network access and privileges based on their role?
☐ Yes ☐ No

13. Does the Applicant have procedures in place to terminate a user's access to the network after they are no longer an employee? ☐ Yes ☐ No

14. Does the Applicant have any servers located outside the United States? ☐ Yes ☐ No
If Yes, where: _____

15. Please identify the Applicant's IT Vendors and Outsource Providers (as applicable):
Anti-Virus: _____
Firewalls: _____
Are firewalls connected securely at all external entry points? ☐ Yes ☐ No
Intrusion Detection/Prevention: _____
Alert Log Monitoring: _____
Data Storage / collocation: _____
Other (please state): _____

16. Does the Applicant have agreements with the Vendors/Outsource Providers listed in response to Question 15 (above) that include indemnification and hold harmless language in the Applicant's favor regarding any data breach, or security or privacy-related claim or loss caused by a failure of the Vendor/Outsource Provider's network security? ☐ Yes ☐ No

17. If the Applicant accepts credit cards for payment from clients/customers, please advise regarding the below:

i. What proportion (%) of the Applicant's gross annual revenues is attributed to payment via credit cards? _____(%)

ii. What proportion of credit card payments are made online compared to in-store at a physical Point of Sale (POS) system?
_____(% from Online/Website sales)
_____(% via physical POS system)

iii. At what level of PCI compliance has the Applicant been certified?

☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4

iv. When was the Applicant's last PCI certification? _____

v. Does the applicant's POS system employ end-to-end encryption? ☐ Yes ☐ No

APPLICANT SIGNER'S NAME: _____

APPLICANT SIGNER'S SIGNATURE: _____

APPLICANT SIGNER'S TITLE: _____

DATE:_____