PHILADELPHIA INSURANCE COMPANIES
A Member of the Tokio Marine Group

One Bala Plaza, Suite 100
Bala Cynwyd, PA 19004

Underwritten by:
Philadelphia Indemnity Insurance Company

CYBER SECURITY LIABILITY RENEWAL APPLICATION – NEW YORK

COVERAGES E., F., AND G. ARE CLAIMS MADE AND REPORTED COVERAGES.

CLAIM EXPENSES UNDER COVERAGES E., F., AND G. ARE INCLUDED WITHIN THE AVAILABLE LIMIT OF INSURANCE. ANY CLAIM EXPENSES PAID UNDER THIS COVERAGE FORM WILL REDUCE THE AVAILABLE LIMITS OF INSURANCE AND MAY EXHAUST THEM COMPLETELY. PLEASE READ THE ENTIRE POLICY CAREFULLY.

Certain terms have specific meaning as defined in the policy form and noted in **bold**. Throughout this Application the words "you" and "your" refer to the **Named Insured** shown in the Declarations, and any other person or organization qualifying as a **Named Insured** under the proposed policy.

SECTION I – GENERAL INFORMATION

Name of Applicant:

Address:

City: State: Zip:

Telephone: Website: www.

Risk Management Contact:

Risk Manager Email:

Please provide a brief description of operations:

Please list all subsidiaries for which coverage is requested under this policy:

To enter more information, please use the Additional information page attached to this application.

	US / Canada	Other Countries	Total
Total number of employees			
Annual sales or revenue	$	$	$
Annual revenue from online sales or services	$	$	$

1. Do you collect, store or process any of the following types of Personally Identifiable Information (PII)?   Yes   No
   Please check all that apply:
   - Bank Account Information
   - Credit Card Numbers
   - Driver's License Information
   - Protected Health Information / Medical Records
   - Social Security Numbers
   - Other: (please specify)

2. Please estimate the total number of Personally Identifiable Information records held:

Insuring Agreement	Requested Limit	Requested Deductible
A. Loss of Digital Assets	$	$
B. Non-Physical Business Interruption & Extra Expense	$	(N/A – Time Retention Applies)
C. Cyber Extortion Threat	$	$
D. Security Event Costs	$	$
E. Network Security & Privacy Liability	$	$
F. Employee Privacy Liability	$	$
G. Electronic Media Liability	$	$
H. Cyber Terrorism Coverage	$	$

SECTION III - LOSS EXPERIENCE

(Explain any "Yes" responses, including corrective actions and damages incurred on the ADDITIONAL INFORMATION page below):

1. Since you last completed an application for the proposed insurance, have you sustained any losses due to unauthorized access, unauthorized use, virus, denial of service attack, electronic media liability, data breach, data theft, fraud, electronic vandalism, sabotage or other similar electronic security events?   Yes   No

2. Since you last completed an application for the proposed insurance, have you experienced any network related business interruption exceeding eight (8) hours other than planned maintenance?   Yes   No

3. Since you last completed an application for the proposed insurance, has anyone alleged that you were responsible for damage to their computer system(s) arising out of the operation of your computer system(s)?   Yes   No

4. Since you last completed an application for the proposed insurance, have you received a complaint or other proceeding (including an injunction or other request for non-monetary relief) arising out of intellectual property infringement, copyright infringement, media content, or advertising material?   Yes   No

5. Since you last completed an application for the proposed insurance, has anyone made a demand, claim, complaint, or filed a lawsuit against you alleging invasion of, or interference with rights of privacy, or the inappropriate disclosure of personally identifiable information (PII)?   Yes   No

6. Since you last completed an application for the proposed insurance, have you been the subject of an investigation or action by any regulatory or administrative agency for privacy-related violations?   Yes   No

SECTION IV – RISK CONTROLS

1. Do you have a firewall?   Yes   No
   a. How often do you review the rules within the firewalls?
   b. When was the last time a rule was removed / deactivated?

2. Do you require your Information Technology Department or outsourced third party vendors/providers to adhere to a software update process, including software patches and anti-virus software definition upgrades?   Yes   No

3. Do you perform virus scans of emails, downloads, and portable devices?   Yes   No

4. Do you restrict access to sensitive client, customer, employee or other third party information?   Yes   No

5. Do you have a process for managing user accounts, including the timely revocation of access for terminated employees and the removal of outdated accounts?   Yes   No

6. Do you have physical security controls in place to restrict access to your computer systems and sensitive paper records? Yes   No

7. Do you have role-based controls or other procedures that address user access to critical and sensitive computer systems, applications, or records? Yes   No

8. Do you have a written business continuity/disaster recovery plan that includes procedures to be followed in the event of a disruptive computer or network incident? Yes   No

9. Are system back-up and recovery procedures tested for all mission-critical systems and performed at least annually? Yes   No

10. Do you have a designated individual or group responsible for information security and compliance operations? Please specify below by checking all that apply:
    Risk Management Department
    Chief Information Officer / Chief Information Security Officer
    Other: (please specify)

11. Is all sensitive customer, client and employee data:
    a. encrypted at rest? Yes   No
    b. encrypted in transit? Yes   No
    c. accessible via mobile devices, laptops or other portable storage media? Yes   No
    If yes, are the mobile devices, laptops or other storage media encrypted? Yes   No

12. How long would it take to restore your operations after a computer attack or other loss/corruption of data?   0-12 Hours   12-24 Hours   24 Hours

13. Are mission-critical transactions and security logs reviewed periodically for suspicious activity? Yes   No
    If yes, how frequently?

14. Have you undergone an information security or privacy compliance evaluation? Yes   No
    If yes, identify who performed the evaluation, the date it was performed, the type of evaluation, and attach a copy of it.

    Were all recommendations implemented and deficiencies corrected? Yes   No
    If no, please explain on the ADDITIONAL INFORMATION page)

15. Do you outsource critical components of your network/computer system or internet access/presence to others? Yes   No
    If yes, check all that apply and name the service provider for each category:

TECH-RELATED SERVICE			
Internet Service Provider	Backup, co-location and data recovery	Financial Services and Payment Processing	Other: "cloud", ASP, SAAS, Etc.
Comcast	AT & T	ADP	Amazon
Verizon	Mozy	Authorize.net	Microsoft
Time Warner	HP	Blackbaud	Google
AT & T	IBM	BA Merchant Services	Go Daddy
Optimum / Cablevision	Iron Mountain	First Data	IBM
Cox	Rackspace	Fiserv	Media Temple
Century Link	Sunguard	Global Payments	Endurance/Bluehost
Windstream	TierPoint	Heartland	Rackspace
Charter	In House	Metavente	Akamai
Road Runner	Other:	Paymentech	Verizon
Level 3		Paypal	SoftLayer
Other:		Square	HostGator
		Stripe	VMWare/Dell/EMC
		Verisign	Salesforce
		Other:	Other:

16.	Do you have a program in place to periodically test your data security controls?	Yes	No	

17.	Do you have written contracts in place to enforce your information security policy and procedures with third party service providers?	Yes	No	

18.	Do such contracts contain hold harmless or indemnification clauses in your favor?	Yes	No	

19.	Do you audit all vendors and service providers who handle or access your data and require them to have adequate security protocols?	Yes	No	

20.	Do you have a document destruction and retention policy?	Yes	No	

21.	Do you monitor your network in real time to detect possible intrusions or abnormalities in the performance of the system?	Yes	No	

SECTION V – PRIVACY CONTROLS

1. Have you achieved compliance with the following: (check all that apply)

PCIDSS (Payment Card Industry Data Security Standard)	Yes	No	N/A
GLBA (Gramm-Leach-Bliley Act)	Yes	No	N/A
HIPAA (Health Insurance Portability and Accountability Act)	Yes	No	N/A

2. Does your hiring process include the following for all employees and independent contractors (check all that apply):

Drug testing	Work history checks
Criminal background checks	Credit history checks
Educational background	Other (specify):

3.	Do you have a current enterprise-wide computer network and information security policy that applies to employees, independent contractors, and third-party vendors?	Yes	No
	If yes, is the information published within the company (e.g. corporate intranet, employee handbook, etc.)?	Yes	No

4.	Are all employees periodically instructed on their specific job responsibilities with respect to information security, such as the proper reporting of suspected security incidents?	Yes	No

5.	Do you have a formal written privacy policy?	Yes	No
	If yes, has the policy been reviewed and approved by legal counsel?	Yes	No

6.	Are your information systems and supporting business procedures prepared to honor customer preferences concerning the opt-out of sharing of non-public, personal information to non-affiliated third parties?	Yes	No

7.	Do you require the transmission of personal customer information such as credit card numbers, contact information, etc., as part of your internet-based services?	Yes	No

SECTION VI – MEDIA LIABILITY CONTROLS

1. Do you have a process to review content or materials (including meta tags) before they are published, broadcasted, distributed, or displayed on your website for the following:

Defamation (Slander or Libel)?	Yes	No
Right to privacy or publicity?	Yes	No
Copyright, trademark or domain name?	Yes	No

2.	Have your products or services been the subject of copyright, patent or trademark infringement allegations?	Yes	No

3.	Does your organization use social media?	Yes	No
a.	Do you monitor postings?	Yes	No
b.	Are there formal procedures for complaints?	Yes	No
c.	Is content reviewed by legal counsel?	Yes	No

ADDITIONAL INFORMATION

This page may be used to provide additional information to any question on this application. Please identify the question number to which you are referring.

_____

Signature   Date

FRAUD STATEMENT AND SIGNATURE SECTIONS

The Undersigned states that they/ them are an authorized representative of the Applicant and declares to the best of their knowledge and belief and after reasonable inquiry, that the statements set forth in this Application (and any attachments submitted with this Application) are true and complete and may be relied upon by Company * in quoting and issuing the policy. If any of the information in this Application changes prior to the effective date of the policy, the Applicant will notify the Company of such changes and the Company may modify or withdraw the quote or binder.

The signing of this Application does not bind the Company to offer, or the Applicant to purchase the policy.
*Company refers collectively to Philadelphia Indemnity Insurance Company and Tokio Marine Specialty Insurance Company

VIRGINIA APPLICANT: READ YOUR POLICY. THE POLICY OF INSURANCE FOR WHICH THIS APPLICATION IS BEING MADE, IF ISSUED, MAY BE CANCELLED WITHOUT CAUSE AT THE OPTION OF THE INSURER AT ANY TIME IN THE FIRST 60 DAYS DURING WHICH IT IS IN EFFECT AND AT ANY TIME THEREAFTER FOR REASONS STATED IN THE POLICY.

FRAUD NOTICE STATEMENTS

APPLICABLE IN NEW YORK: 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 SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION. THIS APPLIES TO AUTO INSURANCE.

NAME (PLEASE PRINT/TYPE)

TITLE
(MUST BE SIGNED BY THE PRESIDENT, BOARD CHAIR, CEO OR EXECUTIVE DIRECTOR)

_____

SIGNATURE

DATE

SECTION TO BE COMPLETED BY THE PRODUCER/BROKER/AGENT

PRODUCER
(If this is a Florida Risk, Producer means Florida Licensed Agent)

AGENCY

PRODUCER LICENSE NUMBER
(If this a Florida Risk, Producer means Florida Licensed Agent)

ADDRESS (STREET, CITY, STATE, ZIP)