

**CyberChoice First Response<sup>sm</sup> Policy  
Data Privacy and Network Security Insurance  
Application**



If a policy is issued, this application will attach to and become part of the policy. Therefore, it is important that all questions are answered accurately.

**NOTICE: THIS IS AN APPLICATION FOR A POLICY THAT CONTAINS CLAIMS MADE COVERAGE. EXCEPT AS OTHERWISE SPECIFIED IN THE POLICY: COVERAGE APPLIES ONLY TO A CLAIM FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD AND WHICH HAS BEEN REPORTED TO THE INSURER IN ACCORDANCE WITH THE APPLICABLE NOTICE PROVISIONS, PROVIDED THAT SUCH NOTICE IS GIVEN NO LATER THAN SIXTY (60) DAYS AFTER THE TERMINATION OF THE POLICY PERIOD. COVERAGE IS SUBJECT TO THE INSURED'S PAYMENT OF THE APPLICABLE RETENTION. DEFENSE EXPENSES ARE APPLIED AGAINST THE RETENTION. FURTHER, PAYMENT OF DEFENSE EXPENSES REDUCES THE LIMITS OF LIABILITY. PLEASE READ THE POLICY CAREFULLY AND DISCUSS THE COVERAGE WITH YOUR INSURANCE AGENT OR BROKER.**

Whenever used in this Application, the term "Applicant" shall mean the entity proposed as the **Named Insured** and any subsidiaries thereof, and the respective directors, officers, trustees, and governors of all such entities.

A. COVERAGE REQUESTED		
Requested Effective Date:	Requested Prior Acts Coverage:	
Requested Coverage Part:	Requested Limit:	Requested Retention:
Data Privacy and Network Security Liability		
Digital Media Liability		
Incident Response Fund		
Cyber Extortion Loss		
Data Restoration Expense		
Business Interruption Loss		Waiting Period (hrs):
Dependent Business Interruption Loss		Waiting Period (hrs):

B. GENERAL INFORMATION			
Name of Applicant:			
Company Type:	Public	Private	Non-Profit Government
Mailing Address:			State of Incorporation:
City:			State and Zip Code:
Year Established:	NAICS Code:	Number of Employees:	
Description of your business:			
Website(s):	IP Range:		
Do you have a Parent Entity?	Yes	No	Parent Entity Address:
Parent Entity name:			
Was the Applicant involved in (or will the Applicant be involved in) any actual or attempted merger, acquisition or divestment?	Past 24 months?	Yes	No
	Next 12 months?	Yes	No
	If yes, please explain:		

<b>C. FINANCIAL INFORMATION</b>			
Please respond based on the Applicant's fiscal year end.	Most Recent Fiscal Year End:	Prior Fiscal Year End:	Projected Fiscal Year End:
Total Assets:			
U.S. Revenue:			
Foreign Revenue:			
% revenue from internet:			
Number of payment card transactions per year:			

<b>D. PREVIOUS INSURANCE</b>						
PRODUCT	INSURER	LIMIT	SIR	POLICY PERIOD	PREMIUM	RETRO DATE

<b>E. PRIOR LOSSES AND INCIDENTS</b>		
Is the Applicant or anyone for whom coverage is proposed aware of any facts, acts, circumstances, or situations that may result in coverage under the insurance policy for which the Applicant is hereby applying?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
In the past 3 years, has the Applicant experienced any network intrusions which resulted in the loss, theft or damage to nonpublic personal information or corporate confidential information?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Has the Applicant experienced any unauthorized intrusions into its network in the past 3 years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
In the past 3 years, has an employee or independent contractor been disciplined for mishandling company data or violating the company's privacy or network security policy?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Has the Applicant notified a data breach or security incident to a local, state, federal or foreign government regulator within the past 3 years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Has the Applicant sustained an unscheduled network outage over the past 3 years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
In the past 3 years, has the Applicant been given notice of potential infringement of another party's intellectual property rights, including but not limited to, patent, copyright, trademark, or domain name registrations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
During the past 3 years, has the Applicant sought coverage for loss under any other insurance policy where such type of loss would be tendered for coverage under the proposed insurance policy for which the Applicant is hereby applying?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>F. The Hartford Cybersecurity Services</b>		
Did the Applicant engage any cybersecurity services available through The Hartford within the last 12 months?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Service Provider:	Service Engaged:	
Total Spend by Applicant:	Contract Term:	
Summary of Results:		
<ul style="list-style-type: none"> <li>• Controls Implemented:</li> <li>• Impact on privacy or information security:</li> <li>• Comments:</li> </ul>		

**G. ASSET IDENTIFICATION AND MANAGEMENT**

1. Does the Applicant have a Chief Privacy Officer or equivalent position? If not, are there any other positions that are responsible for privacy related issues? Position title: _____ % of time spent on privacy related issues: _____%	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
2. Does the Applicant have a Chief Information Security Officer or equivalent position? If not, are there any other positions that are responsible for security related issues? Position title: _____ % of time spent on security related issues: _____%	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
3. Has the Applicant identified and inventoried systems and physical devices (including laptops and mobile devices) within the Applicant's information system?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4. Does the Applicant collect, process, control, use, or share sensitive information? If yes, please check all that apply and provide approximate number of records.  <input type="checkbox"/> Social Security Numbers: _____ <input type="checkbox"/> Healthcare Records: _____ <input type="checkbox"/> Payment Card Information: _____ <input type="checkbox"/> Medical Identification Information: _____ <input type="checkbox"/> Drivers' License Numbers: _____ <input type="checkbox"/> Credit Rating Information: _____ <input type="checkbox"/> Financial Account Numbers: _____ <input type="checkbox"/> User Names and Passwords: _____ <input type="checkbox"/> Other Government ID Numbers: _____ <input type="checkbox"/> Third Party Confidential Data: _____ <input type="checkbox"/> Biometric Data: _____ <input type="checkbox"/> Other: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No
5. Has the Applicant conducted a risk assessment of the assets identified in Question 4? a. Does the risk assessment include an asset classification system to identify assets that require heightened controls? (e.g. public, confidential, critical) b. Has the applicant applied risk-appropriate controls (administrative, physical, or technical) to each class of identified assets based on the risk assessment?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
6. Does the Applicant have a written information security policy? a. Updated within the last: <input type="checkbox"/> 120 Days <input type="checkbox"/> 180 Days <input type="checkbox"/> Year <input type="checkbox"/> Never Updated b. Is the Applicant in compliance with its written information security policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
7. Does the Applicant have an attorney-reviewed privacy policy that governs the collection, use, sharing, and retention of personal information? a. Updated within the last: <input type="checkbox"/> 120 Days <input type="checkbox"/> 180 Days <input type="checkbox"/> Year <input type="checkbox"/> Never Updated b. Is the Applicant in compliance with its privacy policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
8. Does the Applicant provide privacy notices to consumers on its website and mobile applications? a. Have the privacy notices been reviewed by an attorney? b. Are the Applicant's business practices consistent with its privacy notices?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
9. Does the Applicant regularly assess its privacy and security policies for compliance with applicable standards and regulations? (If yes, check all that apply)  <input type="checkbox"/> PCI DSS (version: _____) <input type="checkbox"/> Graham-Leach-Bliley Act <input type="checkbox"/> HIPAA/HITECH <input type="checkbox"/> Identity Theft Red Flags Rule under FACTA <input type="checkbox"/> Other: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No
10. Does the Applicant have and enforce a data retention policy? a. Does the Applicant regularly and properly destroy sensitive data no longer necessary for business purposes? b. Does the Applicant have a process for proper destruction of digital media and non-digital information in compliance with applicable regulations?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No

<b>H. ASSET SECURITY AND PROTECTION</b>		
1. Does the Applicant require approvals to create, disable, or modify information system accounts, including privileged and vendor accounts?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Does the Applicant limit access to information systems, including on mobile devices, by the business need to know and role of users, including employees and vendors?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the Applicant require complex passwords to access Applicant's networks, applications, and user accounts?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. How often do users and vendors have to change passwords to access Applicant's network environment, applications, or user accounts? <input type="checkbox"/> At least every 90 days <input type="checkbox"/> At least every 120 days <input type="checkbox"/> At least every 180 days <input type="checkbox"/> 180 days or more <input type="checkbox"/> No requirements to change passwords		
5. Does the Applicant limit the number of attempts to access a password protected account?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the Applicant deploy multifactor authentication for customers, clients, employees, and vendors to access Applicant's networks, applications, and user accounts?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Does the Applicant implement policies and controls regarding the number of concurrent sessions and session lock or termination?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8. Does the Applicant allow remote access to its network by employees or vendors? <ul style="list-style-type: none"> <li>• Does the Applicant restrict remote access to its network by employees and vendors to Virtual Private Networks?</li> </ul>	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9. Does the Applicant maintain physical access audit logs to server rooms, media storage areas, and data and communication centers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
10. Does the Applicant segment its network to protect sensitive data? a. Does the Applicant have information flow control policies? (e.g. firewalls that specify information transfer rules between connected systems) b. Does the Applicant have a policy and process for restricting transfers of sensitive information within its network?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
11. Does the Applicant conduct background investigations of its new hires and require execution of appropriate access or non-disclosure agreements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12. Does the Applicant conduct training for all employees, including privileged users (network administrators, information systems managers, etc.) regarding their privacy and security responsibilities and the Applicant's privacy, security, and use policies? a. Is the training provided at least on an annual basis to all employees? b. Does the Applicant record employee participation for every training session conducted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
13. Does the Applicant revoke network privileges within 2 business days following an employee's or contractor's termination or resignation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
14. Does the Applicant use encryption to protect sensitive information and its devices? a. Does the Applicant have an encryption key management policy, which includes encryption key rotation? b. Please indicate where the Applicant utilizes encryption: <input type="checkbox"/> data transmitted over external networks <input type="checkbox"/> mobile devices, including laptops <input type="checkbox"/> data transmitted over its network <input type="checkbox"/> data processed, stored, or managed via cloud services <input type="checkbox"/> data at rest <input type="checkbox"/> removable storage media (including backup tapes) <input type="checkbox"/> desktops <input type="checkbox"/> other: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No

15. Protection against Malicious Code:		
a. Does the Applicant deploy commercial grade boundary protection tools, including firewalls?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the Applicant deploy commercial grade anti-virus/malware applications, which are updated and released to all devices within 24 hours?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Is the anti-malware application configured to continuously scan or to perform periodic scans of the information system?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Is the anti-malware application configured to scan files from external sources?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
e. How timely are security patches applied as they become available? <input type="checkbox"/> Within 30 Days <input type="checkbox"/> Within 90 Days <input type="checkbox"/> Within 180 Days <input type="checkbox"/> >180 Days		
16. Does the Applicant have a policy that requires new or updated products, systems, databases, and software to be tested, and assessed for privacy and security issues?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
17. Does the Applicant perform annual assessments for its physical and network security policies and procedures? (e.g. penetration testing by outside vendors)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
18. Does the Applicant utilize data loss prevention tools to identify and monitor sensitive data and to prevent unauthorized transmissions of sensitive data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
19. Does the Applicant utilize software or hardware that is no longer supported or has been identified as end-of-life support by the software or hardware vendor? Please identify such software and hardware and outline any plans for remediation:	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>I. VENDOR MANAGEMENT</b>		
1. Approximately % of operations that are outsourced:		<input type="text"/> %
Please indicated the operation(s) outsourced and the name of the third party vendor(s):		
<input type="checkbox"/> Network Security Service Provider:	<input type="text"/>	
<input type="checkbox"/> Data Storage/Back-up/Recovery:	<input type="text"/>	
<input type="checkbox"/> Systems Development and Maintenance:	<input type="text"/>	
<input type="checkbox"/> Payment Card Processing:	<input type="text"/>	
<input type="checkbox"/> Payment Applications:	<input type="text"/>	
<input type="checkbox"/> Point of Sale Devices:	<input type="text"/>	
<input type="checkbox"/> Payroll Services:	<input type="text"/>	
<input type="checkbox"/> Website Hosting:	<input type="text"/>	
<input type="checkbox"/> Other:	<input type="text"/>	
2. Does the Applicant utilize Cloud services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<input type="checkbox"/> Infrastructure as a Service (IAAS) Provider:	<input type="text"/>	
<input type="checkbox"/> Platform as a Services (PAAS) Provider:	<input type="text"/>	
<input type="checkbox"/> Software as a Services (SAAS) Provider:	<input type="text"/>	
a. Does the Applicant store, process, or otherwise manage Nonpublic Personal Information (NPI) or corporate confidential information through Cloud services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the Applicant have the ability to generate a unique encryption key?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Does the Applicant regularly rotate its encryption keys?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Does the Applicant have the right to audit system and application logs or network security controls of the cloud provider?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
e. Is Applicant's data segregated by physical segmentation (private or hybrid cloud)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
f. Is Applicant's data segregated by network segmentation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

g. Is Applicant's data segregated by application segmentation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the Applicant have a vendor risk assessment program that has been approved by management?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does the Applicant require written contracts for all third party vendors that have access to the Applicant's Computer System or sensitive information? If yes, do the contracts:	<input type="checkbox"/> Yes	<input type="checkbox"/> No
a. specify privacy and security requirements and responsibilities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. require the vendor to defend and indemnify the Applicant for liability arising from any compromise of the information due to the negligence of the vendor?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. require vendors' compliance with applicable privacy and security regulations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does the Applicant require vendors that have access to Applicant's Computer System or sensitive information to carry Data Privacy and Network Security insurance coverage?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the Applicant have a policy requiring an annual audit of the privacy and security practices of vendors to ensure compliance with applicable regulations and requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
• If yes, is the Applicant in compliance with its policy for auditing the privacy and security practices of its vendors?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

#### J. NETWORK MONITORING AND INTRUSION DETECTION

1. Are there positions within the Applicant organization dedicated to monitoring and detecting malicious network activity to ensure accountability? Position title: _____ % of time spent on network monitoring issues: _____%	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Does the Applicant establish, monitor and manage baselines for network operations and expected data flows for users and systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the Applicant review network activity against previously established baseline activity for unusual or abnormal activity?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does the Applicant use intrusion detection or prevention systems, or network monitoring software to monitor network intrusions or unauthorized network activity?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does the Applicant use security information and event management (SIEM) software to analyze and manage network events?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Log Generation, Analysis, Storage, and Monitoring		
a. Does the Applicant generate and collect logs related to network security, e.g. system logs, network logs and security application logs?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the Applicant archive logs on a regular basis as part of standard operations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Does the Applicant have policies and procedures for managing and reviewing logs for unusual network activity or indicators of potential compromise?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Does the Applicant conduct regular audits to confirm logging standards and guidelines are being followed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

#### K. INCIDENT RESPONSE PLANS

1. Does the Applicant have a written incident response plan related to a privacy or network security event?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
a. Does the incident response plan designate roles and responsibilities within the organization during the incident response?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the Applicant train all employees regarding its incident response plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Are employees (re)trained at least every year?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Has the Applicant tested its incident response plan within the last 12 months?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
e. Has the Applicant updated its incident response plan within the last 36 months?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

2. Does the Applicant track and document privacy and information system security events?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>L. DISASTER RECOVERY PLANS (FOR EXTORTION, RESTORATION AND INTERRUPTION COVERAGES)</b>		
1. When did the Applicant last test its written business continuity and disaster recovery plans for an IT related event? <input type="checkbox"/> <1 Year ago <input type="checkbox"/> < 3 Years ago <input type="checkbox"/> > 3 Years ago <input type="checkbox"/> Never <input type="checkbox"/> Applicant has no plans		
2. Is there a position responsible for the development, maintenance, and testing of the above plans? Position title: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. How long would it take to restore the Applicant's operations after a network attack or unplanned system outage? <input type="checkbox"/> 0-12 Hours <input type="checkbox"/> 12-24 Hours <input type="checkbox"/> 24-48 Hours <input type="checkbox"/> More than 48 Hours <input type="checkbox"/> Unknown		
4. Does the Applicant backup system-level and user level information and data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
a. Are backup tapes stored securely in an alternative site and properly purged after the retention period?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. How often does the Applicant backup system-level and user level information? <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly <input type="checkbox"/> Never		
5. Does the Applicant have an alternate storage site that maintains duplicate copies of information and data in the event that the primary site becomes unavailable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the Applicant maintain an alternate processing site to maintain business function in the event that the primary site becomes unavailable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Does the Applicant employ tools and controls to limit the effect of denial of service attacks? (e.g. utilizing boundary protection devices; creating sufficient capacity and service redundancies; managing network and storage capacities)	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>M. DIGITAL MEDIA COVERAGE (FOR DIGITAL MEDIA COVERAGE ONLY)</b>		
1. Does the Applicant have policies and procedures for editing or removing infringing or offensive content from its websites, social media platforms, or any other media or materials published or distributed by or on behalf of the Applicant?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. Describe the activity or planned activity (next 12 months) on the Applicant's websites: (Check all that apply) <input type="checkbox"/> provides information and content about the Applicant's products and services <input type="checkbox"/> displays content aggregated from third party sources <input type="checkbox"/> allows posting of content by visitors and/or employees on the website (e.g. forums, boards, chatrooms) <input type="checkbox"/> manages forum or listing for the buying /selling of goods and services <input type="checkbox"/> engages in financial transactions (payment card or virtual currency transactions) <input type="checkbox"/> provides legal, financial, technology, health or medical advice <input type="checkbox"/> has files for download <input type="checkbox"/> provides gambling or adult entertainment services <input type="checkbox"/> links or embeds content from media or networking sites (e.g. YouTube, Hulu, LinkedIn)		
3. Does the Applicant manage or maintain a presence on any social media platforms?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
a. Does the Applicant have a formal social media policy that has been approved by management?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the Applicant require employees to acknowledge receipt of the Applicant's social media policy?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Does the Applicant train employees regarding its social media policy?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Does the Applicant review content posted on its social media platforms for legal and regulatory issues?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does the Applicant tailor, target, or market its websites, media, products, or services to children?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
a. Does the Applicant collect data about children who use its websites or other internet services?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the Applicant have a process for obtaining appropriate consent prior to		

collection, use, or sharing of that data in compliance with applicable regulations?

Yes

No

5. Does the Applicant have written policies and procedures for clearing and protecting intellectual property rights for content displayed or disseminated on its internet media platforms, including websites, e-mail marketing, mobile apps, or social media?

Yes

No

a. Does the Applicant acquire all necessary rights, licenses, releases, and consent for its internet media content?

Yes

No

b. Does the Applicant acquire written permission from sites to which it links?

Yes

No

c. Does the Applicant protect intellectual property rights within employee and third party contractor agreements?

Yes

No

d. Does the Applicant regularly protect its intellectual property rights through nondisclosure agreements?

Yes

No

e. Does the Applicant screen all trademarks used by the Applicant for infringement prior to first use?

Yes

No

f. Please indicate whether the Applicant screens internet content, including postings and submissions by visitors, for the following:

Copyright and trademark infringement

Defamation

Domain name infringement

Privacy violations

### **ADDITIONAL APPLICATION MATERIALS**

At the discretion of the Insurer, and as is relevant to the requested coverage(s), the following materials may be required.

- The most recent fiscal year-end financial statements;
- Any specific claim information related to prior losses;
- Explanations to all questions that require additional clarification;
- The latest edition of the Applicant's privacy policy and/or notice;
- The latest edition of the Applicant's written information security policy;
- A copy of service agreements used with third parties providing services or platforms to/for the Applicant.

**IT IS UNDERSTOOD AND AGREED THAT ANY REPRIMAND, DISCIPLINARY OR CRIMINAL ACTIONS; LITIGATION, CLAIM, ARBITRATION, CIVIL, CRIMINAL, ADMINISTRATIVE OR REGULATORY ACTION OR PROCEEDING; OR KNOWLEDGE OR INFORMATION, ANY CLAIM OR ACTION FOR, BASED UPON, ARISING FROM OR IN ANY WAY RELATED THERETO IS EXCLUDED FROM THIS PROPOSED COVERAGE. THE INFORMATION PROVIDED IN THIS APPLICATION IS FOR UNDERWRITING PURPOSES ONLY AND DOES NOT CONSTITUTE NOTICE TO THE COMPANY OF A CLAIM OR POTENTIAL CLAIM UNDER ANY POLICY. IF YOU INTEND TO NOTICE A CLAIM OR POTENTIAL CLAIM FOR POSSIBLE COVERAGE, PLEASE COMPLY WITH THE NOTICE OF CLAIM CONDITIONS/PROVISIONS FOUND IN YOUR POLICY**

The Undersigned declares that the person(s) and entity(ies) proposed for this insurance understands that:

- With respect to Liability Coverages, the **Policy** shall apply only to **Claims** made during the **Policy Period** or Extended Reporting Period (if applicable);
- The limit of liability contained in the **Policy** shall be reduced, and may be completely exhausted, by **Defense Expenses**, and, in such event, the Insurer shall not be liable for **Defense Expenses** or for the amount of any judgment or settlement to the extent that such cost exceeds the limit of liability in the **Policy**; and
- **Defense Expenses** that are incurred shall be applied against the retention amount.

### **FRAUD WARNING STATEMENTS**

**ATTENTION ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, RHODE ISLAND AND WEST VIRGINIA APPLICANTS: ANY PERSON WHO KNOWINGLY (OR WILLFULLY IN MARYLAND) PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY (OR WILLFULLY IN MARYLAND) PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.**

**ATTENTION 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 POLICY HOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICY HOLDER 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.**

**ATTENTION 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.**

**ATTENTION KANSAS APPLICANTS: INSURANCE FRAUD IS A CRIMINAL OFFENSE IN KANSAS. A " FRAUDULENT INSURANCE ACT " MEANS AN ACT COMMITTED BY ANY PERSON WHO, KNOWINGLY AND WITH INTENT TO DEFRAUD, PRESENTS, CAUSES TO BE PRESENTED OR PREPARES WITH KNOWLEDGE OR BELIEF THAT IT WILL BE PRESENTED TO OR BY AN INSURER, PURPORTED INSURER, BROKER OR ANY AGENT THEREOF, ANY WRITTEN ELECTRONIC, ELECTRONIC IMPULSE, FACSIMILE, MAGNETIC, ORAL, OR TELEPHONIC COMMUNICATION OR STATEMENT AS PART OF, OR IN SUPPORT OF, AN APPLICATION FOR THE ISSUANCE OF, OR THE RATING OF AN INSURANCE POLICY FOR PERSONAL OR COMMERCIAL INSURANCE, OR A CLAIM FOR PAYMENT OR OTHER BENEFIT PURSUANT TO AN INSURANCE POLICY FOR COMMERCIAL OR PERSONAL INSURANCE WHICH SUCH PERSON KNOWS TO CONTAIN MATERIALLY FALSE INFORMATION CONCERNING ANY FACT MATERIAL THERETO; OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO.**

**ATTENTION KENTUCKY, 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.**

**ATTENTION 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 MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.**

**ATTENTION NEW MEXICO APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO CIVIL FINES AND CRIMINAL PENALTIES.**

**ATTENTION NEW HAMPSHIRE AND NEW JERSEY APPLICANTS: ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION TO THE BEST OF HER/HIS KNOWLEDGE ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.**

**ATTENTION OKLAHOMA APPLICANTS: WARNING, ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.**

**ATTENTION OREGON APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD OR SOLICIT ANOTHER TO DEFRAUD AN INSURER: (1) BY SUBMITTING AN APPLICATION OR; (2) FILING A CLAIM CONTAINING A FALSE STATEMENT AS TO ANY MATERIAL FACT MAY BE VIOLATING STATE LAW.**

**ATTENTION NEW YORK 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 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.**

THE UNDERSIGNED AUTHORIZED OFFICER OF THE APPLICANT DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AUTHORIZED OFFICER AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS AND/OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE. THE "EFFECTIVE DATE" IS THE DATE THE COVERAGE IS BOUND OR THE FIRST DAY OF THE CURRENT POLICY PERIOD, WHICHEVER IS LATER. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED AND IT WILL BE ATTACHED TO AND BECOME A PART OF THE POLICY. ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF.

**THIS PAGE CONTAINS STATE SPECIFIC LANGUAGE OR REQUIREMENT FOR APPLICANTS RESIDING IN THE FOLLOWING STATES: Florida, Iowa, Maine and New Hampshire**

**Applicable to Maine applicants only**

THE UNDERSIGNED AUTHORIZED OFFICER OF THE APPLICANT DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AUTHORIZED OFFICER AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS. THE "EFFECTIVE DATE" IS THE DATE THE COVERAGE IS BOUND OR THE FIRST DAY OF THE CURRENT POLICY PERIOD, WHICHEVER IS LATER. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED AND IT WILL BE ATTACHED TO AND BECOME A PART OF THE POLICY. ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF. THIS APPLICATION MUST BE SIGNED BY THE CHAIRMAN OF THE BOARD, CHIEF EXECUTIVE OFFICER, CHIEF FINANCIAL OFFICER OR THE PRESIDENT OF THE COMPANY.

**Applicable to New Hampshire applicants only**

THE UNDERSIGNED AUTHORIZED OFFICER OF THE APPLICANT DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE TO THE BEST OF HER/HIS KNOWLEDGE. THE UNDERSIGNED AUTHORIZED OFFICER AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS AND/OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE. THE "EFFECTIVE DATE" IS THE DATE THE COVERAGE IS BOUND OR THE FIRST DAY OF THE CURRENT POLICY PERIOD, WHICHEVER IS LATER. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED AND IT WILL BE ATTACHED TO AND BECOME A PART OF THE POLICY. ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF. THIS APPLICATION MUST BE SIGNED BY THE CHAIRMAN OF THE BOARD, CHIEF EXECUTIVE OFFICER, CHIEF FINANCIAL OFFICER OR THE PRESIDENT OF THE COMPANY.

Signature of Applicant's Executive Officer (CEO, CFO, CIO, President, or General Counsel)
Print Name:
Title:
Date:

Signature of Broker/Agent:
Print name:
Title:
Date:

Name of Producer (Required in FL, IA, NH only):
Address:
Date:

Producer License # (Required in NH only):
Name of Agency:
Producer Signature (Required in NH only):