Travelers Casualty and Surety Company of America *(not applicable in Guam, Puerto Rico or Virgin Islands)*
Travelers Casualty and Surety Company *(only applicable in Guam, Puerto Rico and Virgin Islands)*

NOTICE

ALL THIRD PARTY LIABILITY INSURING AGREEMENTS FOR WHICH APPLICATION IS MADE APPLY, SUBJECT TO THEIR TERMS, ONLY TO CLAIMS FIRST MADE OR DEEMED MADE AGAINST INSUREDS DURING THE POLICY PERIOD OR ANY EXTENDED REPORTING PERIOD, IF APPLICABLE. THE LIMIT OF LIABILITY AVAILABLE TO PAY LOSSES WILL BE REDUCED BY THE AMOUNTS INCURRED AS DEFENSE EXPENSES, AND DEFENSE EXPENSES WILL BE APPLIED AGAINST THE RETENTION AMOUNT. THE COMPANY HAS NO DUTY TO DEFEND ANY CLAIM UNLESS DUTY–TO-DEFEND COVERAGE IS SPECIFICALLY PROVIDED.

Applicant means all corporations, organizations or other entities, including subsidiaries, proposed for this insurance.

I. GENERAL INFORMATION

1. Name of **Applicant** : _____

    Mailing Address: _____

    City, State, ZIP Code: _____

    Year Established: _____

    Website Home Page Address(es): _____

    Applicant Company Type: ☐ Public   ☐ Private   ☐ Non-Profit   ☐ Government

    ☐ Other (describe)_____

    Description of **Applicant's** Operations: _____

    Applicant's Standard Industrial Classification (SIC) Code if known (4 digit number): _____

II. ORGANIZATION/FINANCIAL INFORMATION

1. Subsidiary Information:

Name	Description of Operations	Website Address

Attach a separate sheet if necessary.

2. Are significant changes in the nature or size of the **Applicant's** business anticipated over the next 12 months, or have there been any such changes in the past 12 months?   Yes ☐ No ☐
    If Yes, please explain: _____

3. Total number of **Applicant's** employees (full and part time including leased, seasonal and temporary): _____

4. Assets/Revenues:

Indicate the following as it relates to the Applicant's fiscal year end (FYE): *(Please indicate negative figures with " ( )" or "-" as appropriate)*	Most Recent FYE (Month/Year) (_____/_____)	Prior FYE (Month/Year) (_____/_____)	Projected FYE (Month/Year) (_____/_____)
Total Assets	$	$	$
Total Revenue	$	$	$
Total U.S. Revenue	$	$	$

Indicate the following as it relates to the Applicant's fiscal year end (FYE): *(Please indicate negative figures with "( )" or "-" as appropriate)*	Most Recent FYE (Month/Year) (____/____)	Prior FYE (Month/Year) (____/____)	Projected FYE (Month/Year) (____/____)
Total Foreign Revenue	$	$	$
Estimated percentage of revenue derived from or dependent upon website or internet	%	%	%

III.   REQUESTED INSURANCE TERMS/CURRENT INSURANCE INFORMATION

1. Complete the following table for coverages, limits and retentions requested:

Insuring Agreement	Requested Limit	Requested Retention
A. Network and Information Security Liability (Required)	$	$
B. Communications and Media Liability	$	$
C. Regulatory Defense Expenses	$	$
D. Crisis Management Event Expenses	$	$
E. Security Breach Remediation and Notification Expenses	$	$
F. Computer Program and Electronic Data Restoration Expenses	$	$
G. Computer Fraud	$	$
H. Funds Transfer Fraud	$	$
I. E-Commerce Extortion	$	$
J. Business Interruption and Additional Expenses	$	Waiting Period in Hours

Proposed effective date: _____

2. What is the **Applicant's** preference for defense coverage with respect to Insuring Agreements A., B., and C.?   Duty to Defend ☐   Reimbursement ☐

3. If **Applicant** currently has insurance for Errors and Omissions Liability, Network and Security Liability or Media Liability, please provide the following information:

Policy Period	Insurance Company	Limit	Deductible	Retroactive Date	Premium
		$	$		$
		$	$		$

Expiring policy number(s): _____

4.   Within the past 3 years, have any of the coverages or similar coverages been declined, cancelled or nonrenewed? **(Not applicable in Missouri)**   Yes ☐   No ☐
     If Yes, please provide details: _____

_____

IV.   NETWORK SECURITY

SYSTEMS

1. Does the **Applicant** have a designated Chief Security Officer as respects computer systems?   Yes ☐   No ☐
    If No, please indicate what position is responsible for computer security: _____

2. Does the **Applicant** have a formal program in place to test or audit network security controls?   Yes ☐   No ☐

    a. How often are internal audits performed?   _____

    b. How often are outside/third party audits performed?   _____

3. Does the **Applicant** use firewall technology?   Yes ☐   No ☐

4. Does the **Applicant** use anti-virus software? Yes ☐ No ☐

    a. Is anti-virus software installed on all of the **Applicant's** computer systems, including laptops, personal computers, and networks? Yes ☐ No ☐

5. Does the **Applicant** use intrusion detection software to detect unauthorized access to internal networks and computer systems? Yes ☐ No ☐

6. Is it the **Applicant's** policy to upgrade all security software as new releases or improvements become available? Yes ☐ No ☐

7. Does the **Applicant** provide remote access to its network? Yes ☐ No ☐

    a. Is remote access restricted to Virtual Private Networks (VPNs)? Yes ☐ No ☐

8. Is a multi-factor authentication process (multiple security measures used to reliably authenticate/verify the identity of a customer or other authorized user) or a layered security approach required to access secure areas of **Applicant's** website? Yes ☐ No ☐
Please describe authentication/verification methods used: _____

_____

9. Does the **Applicant** send or accept financial transactions intended for deposit, via the use of remote deposit capture technology (e.g. RDC – Remote Deposit Capture)? Yes ☐ No ☐

10. With respect to computer systems functionality, does the **Applicant** have:

    a. A disaster recovery plan? Yes ☐ No ☐

    b. A business continuity plan? Yes ☐ No ☐

    c. An incident response plan for network intrusions and virus incidents? Yes ☐ No ☐

    How often are such plans tested? _____

11. Does the **Applicant** have secondary computer system or site available if the primary resource becomes inoperative? Yes ☐ No ☐

    a. How long before the secondary resources become operational? _____

    b. What percentage of normal system operations can be handled via the secondary resources? _____

12. Is all valuable/sensitive data backed-up by the **Applicant** on a daily basis? Yes ☐ No ☐
If No, please describe exceptions: _____

_____

PERSONNEL, POLICIES AND PROCEDURES

1. Does the **Applicant** conduct training regarding security issues and procedures for employees that utilize computer systems? Yes ☐ No ☐

2. Does the **Applicant** publish and distribute written computer and information systems policies and procedures to its employees? Yes ☐ No ☐

3. Does the **Applicant** terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? Yes ☐ No ☐

4. Does the **Applicant** have a formal documented procedure in place regarding the creation and periodic updating of passwords used by employees or customers? Yes ☐ No ☐

V.   INFORMATION SECURITY

1. Does the **Applicant** collect, receive, process, transmit, or maintain private, sensitive, or personal information from third parties (i.e. customers, clients, patients) as part of its business activities? Yes ☐ No ☐
If Yes, please indicate what type:

☐ Credit/Debit Card Data   ☐ Medical Information   ☐ Bank Accounts and Records
☐ Social Security Numbers   ☐ Employee/HR Information   ☐ Customer Information
☐ Intellectual Property of others   ☐ Other _____

a. Does the **Applicant** have written procedures in place to comply with laws governing the handling or disclosure of such information, including any applicable Red Flag Rules? Yes ☐ No ☐

b. Does the **Applicant** share private, sensitive, or personal information gathered from customers (by the **Applicant** or others) with third parties? Yes ☐ No ☐

2. At any one time, approximately how many individual records containing one or more items of the information listed above does the **Applicant** have stored?

☐ <1,000
☐ 1,000 to 10,000
☐ 10,001 to 100,000
☐ 100,001 to 500,000
☐ 500,001 to 1,000,000

☐ 1,000,001 to 3,000,000
☐ 3,000,001 to 5,000,000
☐ 5,000,001 to 7,000,000
☐ 7,000,001 to 10,000,000
☐ >10,000,000

3. Is user-specific, private, sensitive or confidential information stored on **Applicant's** server(s) encrypted? Yes ☐ No ☐

4. Is user-specific, private, sensitive or confidential information stored on portable communications equipment (e.g., laptops, BlackBerry devices, PDA's, USB Flash Drives, or other portable devices)? Yes ☐ No ☐

a. If yes, does **Applicant** have a company policy or procedure for the secure care, handling and storage of private, sensitive or confidential information on portable communications devices? Yes ☐ No ☐

b. If yes, what percentage of user-specific, private, sensitive or confidential information stored on portable communications devices is encrypted? _____ %

5. Does the **Applicant** require service providers who may have access to the **Applicant's** confidential information or personally identifiable information to demonstrate adequate security policies and procedures? Yes ☐ No ☐

a. Are service providers required by contract to indemnify the **Applicant** for harm arising from a breach of the provider's security? Yes ☐ No ☐

VI.   WEBSITE AND CONTENT INFORMATION

Website (Check all that apply)	Current	Within Next 12 Months
Information website only provides general information about the **Applicant's** products/services	☐	☐
Accessible website has log-in capabilities allowing access to secure or restricted content (e.g., accounts, subscriptions, or profiles) and/or allows user to upload or download secure data	☐	☐
Transactional website allows orders or purchases using credit card, debit card, or bill-pay payment	☐	☐
View account balances or statements	☐	☐
Transfer funds between accounts	☐	☐
Bill payment	☐	☐

1. Does **Applicant's** website contain, disseminate, employ or allow the following?
Please check all that apply:

☐ Music/Sound clips
☐ Movies/Movie clips
☐ Sweepstakes or coupons

☐ Chat Rooms/Message Boards/Blogs
☐ Advertising of others
☐ Sexually explicit material

☐ Executable programs or shareware
☐ Interactive gaming/games of chance
☐ Content specifically targeted at minors

2. Does the **Applicant** have a written intellectual property clearance procedure for content disseminated via the **Applicant's** website? Yes ☐ No ☐

Do the procedures include the following:

a. Review of content by qualified attorney? Yes ☐ No ☐

b. Screening the content for the following:

i. Disparagement issues? Yes ☐ No ☐

ii. Copywriting infringement? Yes ☐ No ☐

iii   Trademark infringement?   Yes ☐ No ☐

iv. Invasion of privacy?   Yes ☐ No ☐

c. Obtaining agreements with outside developers or consultants that include provisions granting the **Applicant** ownership of the intellectual property rights and business methods incorporated into any work for hire performed by or on behalf of the **Applicant?**   Yes ☐ No ☐

d. Requiring employees and independent contractors to sign a statement that they will not use previous employers' or clients' trade secrets or other intellectual property?   Yes ☐ No ☐

e. Obtaining written permission of any website the **Applicant** links to or frames?   Yes ☐ No ☐

3. If the **Applicant** does not have a process to review all content prior to posting, please describe procedures to avoid the posting of improper or infringing content: _____

_____

_____

4. Does **Applicant** have a formal procedure for editing or removing controversial, offensive or infringing material from material distributed, broadcast or published by or on behalf of the **Applicant?**   Yes ☐ No ☐

5. Does **Applicant** collect data about children who use your website?   Yes ☐ No ☐
If Yes, please describe the method used to obtain parental permission: _____

_____

6. Does the **Applicant** have a procedure for responding to allegations that content created, displayed or published by the **Applicant** is libelous, infringing, or in violation of a third party's privacy rights?   Yes ☐ No ☐

7. Has the **Applicant** screened all trademarks used by the **Applicant** for infringement with existing trademarks prior to first use?   Yes ☐ No ☐

a. Has the **Applicant** acquired any trademarks from others in the past 3 years?   Yes ☐ No ☐
If Yes, were acquired trademarks screened for infringement?   Yes ☐ No ☐

VII.   LOSS INFORMATION

In the past 3 years:

1. Has the **Applicant** ever received any claims or complaints, or been subject to any government action, investigation or subpoena with respect to allegations of failing to prevent unauthorized access to confidential information, failing to notify appropriate individuals of any such unauthorized access or failing to allow authorized users access to the **Applicant's** computer systems?   Yes ☐ No ☐

2. Has the **Applicant** ever received any claims or complaints, or been subject to any government action, investigation or subpoena with respect to allegations that any content disseminated on or via the **Applicant's** websites or company email, infringed on the intellectual property rights of another party or caused harm to the reputation of another party?   Yes ☐ No ☐

If question 1 or 2 is answered Yes, provide details below of each claim, complaint, allegation or incident, including costs, losses or damages incurred or paid, any corrective procedures to avoid such allegations in the future and any amounts paid as a loss under any insurance policy.

Date of Such Claim/Complaint	Nature of Claim/Complaint	Amount Paid for Defense	Amount Sought or Paid for Damages	Covered by Insurance?	Corrective Procedures Implemented	Current Status
		$	$	Yes ☐ No ☐		
		$	$	Yes ☐ No ☐		
		$	$	Yes ☐ No ☐		

To enter more information, please attach a separate page to the Application.

3. Has the **Applicant** ever experienced an extortion attempt or demand with respect to its computer systems, or suffered a loss of money, securities or other property due to fraud

committed by means of unauthorized or fraudulently entered computer instructions or code by someone other than an employee?   Yes ☐ No ☐

If Yes, please provide details: _____

_____

4. Has the **Applicant** suffered any known intrusions (i.e., unauthorized access or security breach) or denial of service attacks which impaired the functionality of its computer systems?   Yes ☐ No ☐

If Yes, please provide details: _____

_____

5. Is the **Applicant** or any person proposed for this insurance aware of any fact, circumstance, situation, event or act that reasonably could give rise to a claim against them under the insurance policy for which the **Applicant** is applying?   Yes ☐ No ☐

If Yes, please provide details: _____

_____

*With respect to the information required to be disclosed in response to the questions above, the proposed insurance will not afford coverage for any claim arising from any fact, circumstance, situation, event or act about which any executive officer of the **Applicant** had knowledge prior to the issuance of the proposed policy, nor for any person or entity who knew of such fact, circumstance, situation, event or act prior to the issuance of the proposed policy.*

VIII.   REQUIRED ATTACHMENTS

- Most current audited or annual financial statements if annual revenues exceed $10,000,000 or requested Limit of Liability for Network and Information Security Liability coverage exceeds $3,000,000.

*If additional space is needed to address certain questions, attach additional sheets on **Applicant's** letterhead as necessary.*

IX.   COMPENSATION NOTICE

Important Notice Regarding Compensation Disclosure

For information about how Travelers compensates independent agents, brokers, or other insurance producers, please visit this website: http://www.travelers.com/w3c/legal/Producer_Compensation_Disclosure.html

If you prefer, you can call the following toll-free number: 1-866-904-8348. Or you can write to us at Travelers, Enterprise Development, One Tower Square, Hartford, CT 06183.

X.   FRAUD WARNINGS

Attention: Insureds in Arkansas, D.C., Louisiana, Maryland, New Mexico, and Rhode Island
Any person who knowingly (and willfully in D.C. and MD) presents a false or fraudulent claim for payment of a loss or benefit or who knowingly (and willfully in D.C. and MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Attention: Insureds in Colorado
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.

Attention: Insureds in Florida
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: Insureds in Kentucky, New Jersey, New York, Ohio, and Pennsylvania
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.)

> ***Attention: Insureds in Maine, Tennessee, Virginia, and Washington***
> 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.

XI.   SIGNATURE SECTION

THE UNDERSIGNED AUTHORIZED REPRESENTATIVE (PRESIDENT, CEO, CHIEF INFORMATION/SECURITY OFFICER OR OTHER OFFICER ACCEPTABLE TO TRAVELERS) OF THE APPLICANT DECLARES THAT TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS SET FORTH IN THE ATTACHED TRAVELERS NEW BUSINESS OR RENEWAL APPLICATION FOR INSURANCE ARE TRUE AND COMPLETE AND MAY BE RELIED UPON BY TRAVELERS. IF THE INFORMATION IN ANY APPLICATION CHANGES PRIOR TO THE INCEPTION DATE OF THE POLICY, THE APPLICANT WILL NOTIFY THE COMPANY OF SUCH CHANGES, AND THE COMPANY MAY MODIFY OR WITHDRAW ANY OUTSTANDING QUOTATION. THE COMPANY IS AUTHORIZED TO MAKE INQUIRY IN CONNECTION WITH THIS APPLICATION.

THE SIGNING OF THIS APPLICATION DOES NOT BIND THE COMPANY TO OFFER, NOR THE APPLICANT TO PURCHASE, THE INSURANCE. IT IS AGREED THAT THIS APPLICATION, INCLUDING ANY MATERIAL SUBMITTED THEREWITH, SHALL BE THE BASIS OF THE INSURANCE AND SHALL BE, IN ALL STATES OTHER THAN NC AND UT, CONSIDERED PHYSICALLY ATTACHED TO AND PART OF THE POLICY, IF ISSUED. THE COMPANY WILL HAVE RELIED UPON THIS APPLICATION, INCLUDING ANY MATERIAL SUBMITTED THEREWITH, IN ISSUING THE POLICY.

REPRODUCED SIGNATURES, INCLUDING PHOTOCOPIES, WILL BE TREATED AS ORIGINAL.

_____   _____
Signature * of **Applicant's** Authorized Representative   Name (Printed)
(President, CEO or Chief Information/Security Officer)

_____   _____
Title   Date

*IF YOU ARE ELECTRONICALLY SUBMITTING THIS APPLICATION TO TRAVELERS, APPLY YOUR ELECTRONIC SIGNATURE TO THIS FORM BY CHECKING THE ELECTRONIC SIGNATURE AND ACCEPTANCE BOX BELOW. BY DOING SO, YOU HEREBY CONSENT AND AGREE THAT YOUR USE OF A KEY PAD, MOUSE, OR OTHER DEVICE TO CHECK THE ELECTRONIC SIGNATURE AND ACCEPTANCE BOX CONSTITUTES YOUR SIGNATURE, ACCEPTANCE, AND AGREEMENT AS IF ACTUALLY SIGNED BY YOU IN WRITING AND HAS THE SAME FORCE AND EFFECT AS A SIGNATURE AFFIXED BY HAND.

AUTHORIZED REPRESENTATIVE'S ELECTRONIC SIGNATURE AND ACCEPTANCE ☐

XII.   PRODUCER INFORMATION (ONLY REQUIRED IN FLORIDA, IOWA, AND NEW HAMPSHIRE):

_____   _____
Producer Signature   Producer Name (Printed)

_____   _____   _____
Agency Name   Agency Code   License Number