Instructions for Using Editable Applications and Important Legal Information:

1. Save the document to your local computer.
2. Complete the application by providing your responses in the areas provided; utilize the tab key to move ahead to the next field.
3. If there is not enough space for any particular question, please include the full response in an additional attachment to your application, as you would if you were completing a paper-based application.
4. When you have completed the application, please verify the application for accuracy and completeness before signing the application and forwarding the application to your agent or broker. Do not forward applications directly to Chubb unless you are an agent or broker.
5. If you choose to sign the application with a wet signature, please print the final application, sign the application in ink and forward the application to your agent or broker with any necessary supporting materials.
6. If you apply your signature to this form electronically, you hereby consent and agree that your use of a key pad, mouse or other device to click the "I Agree" button 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. Further, you agree that the lack of a certification authority or other third party verification will not in any way affect the validity or enforceability of your signature or any resulting contract. You can apply your signature electronically by clicking on the signature field. Once all signatures have been applied, forward the application to your agent or broker via email. Any necessary supporting materials should be sent via email or postal service to your agent or broker.

If you experience technical difficulties utilizing the document, please contact the Chubb Help Desk at 1-877-747-5266, "Option 2".
For all other inquiries please contact your agent or broker. If you are an agent or broker, please contact your local Chubb representative. The document is provided for licensed insurance agents and brokers and their clients only.

IF YOU ARE ACCESSING THE DOCUMENT FROM A VENUE OTHER THAN WWW.CHUBB.COM, BY YOUR USE OF THE DOCUMENT, YOU ARE AGREEING TO THE FOLLOWING, IF YOU DO NOT AGREE, DO NOT USE THE ELECTRONIC DOCUMENT:
* Chubb does not warrant that the document will be free from viruses. You assume the entire cost of any necessary service, repair or correction.
* The privacy of communication over the Internet cannot be guaranteed, because the Internet is not a secure medium. Chubb does not assume any responsibility for any harm, loss, or damage you may experience or incur by the sending of personal or confidential information over the Internet.
* Chubb is not responsible for any versions of the document that have been manipulated, altered or revised from the version of the document that appears on www.Chubb.com. Do not post the document on the Internet.

I Agree

I. NAME, ADDRESS AND CONTACT INFORMATION:

1. Name of **Applicant**: _____

2. Address of **Applicant**: _____

   City: _____ State: _____ Zip Code: _____ Telephone: _____

3. **Applicant's** Web Site: _____

4. Name and Address (if different than above) of Primary Contact (Executive Officer authorized to receive notices and information regarding the proposed policy):

   Name: _____ Title: _____ Address: _____

   City: _____ State: _____ Zip Code: _____ Telephone: _____ e-Mail: _____

II. INSURANCE INFORMATION:

1. Please indicate below, by placing an "X" in the box, which coverages are being requested. If coverage is currently purchased, please indicate current limits and current carrier. If coverage is currently not purchased, please so indicate.

Coverage Requested	Limit of Liability Requested	Retention Requested	Limit of Liability Currently Purchased	Current Insurer
CyberLiability	$	$	$	
Optional Coverages:				
☐ Privacy Notification Expenses	$	$	$	
☐ Crisis Management Expenses	$	$	$	
☐ E-Business Interruption and Extra Expenses	$	$	$	

☐ E-Theft Loss	$	$	$	
☐ E-Communication Loss	$	$	$	
☐ E-Threat Expenses	$	$	$	
☐ E-Vandalism Expenses	$	$	$	
☐ Reward Expenses	$	$	$	

2. Policy Period Requested:
From _____ to _____ both days at 12:01 a.m. at the principal address of the Parent Organization.

III. GENERAL RISK INFORMATION:

General Information

1. Does the **Applicant** anticipate in the next twelve (12) months establishing or entering into any related or unrelated ventures which are a material change in operations? ☐ Yes ☐ No

   If "Yes", please provide full details on a separate sheet.

2. Please complete the following information for the **Applicant**:

	Prior Year	Current Year	Projected Year
a. Number of Employees			
b. Total Assets			
c. Gross Revenues			
d. Gross Revenue from on-line sales or services			

3. How many servers does the **Applicant** either own or otherwise have dedicated to their use? _____

4. What is the **Applicant's** total number of IP addresses? _____

5. Does the **Applicant** collect, store or process personally identifiable or other confidential information? ☐ Yes ☐ No

   If "Yes", how many records are held, including the **Applicant's** prospective, current and former customers and employees? _____

6. Is the **Applicant** subject to any of the following:

   (a) HIPAA Privacy and Security Rules? ☐ Yes ☐ No

   (b) The Payment Card Industry (PCI) Security Standard? ☐ Yes ☐ No

   If "Yes", complete PCI section of this CyberSecurity New Business Application.

   (c) The Gramm, Leach, Bliley Act? ☐ Yes ☐ No

   (d) Red Flags Rule? ☐ Yes ☐ No

   (e) Any other Federal or State law or regulation concerning privacy or the safeguarding of personally identifiable or other confidential information (other than state "breach notification" laws)? ☐ Yes ☐ No

If "Yes", please indicate what law(s) or regulation(s): _____

If "Yes", to any of the above in Question 6, is the **Applicant** compliant with the selected rules and standards? ☐ Yes ☐ No

If "No", please explain the **Applicant's** lack of compliance: _____

7. Does the **Applicant** process or store personally identifiable or other confidential information for third parties? ☐ Yes ☐ No

   If "Yes", please attach an explanation.

8. Does the **Applicant** shred all written or printed personally identifiable or other confidential information when it is being discarded? ☐ Yes ☐ No

PCI Compliance

(Please answer the questions in this section if the Applicant is subject to the Payment Card Industry Security Standard)

1. How many credit or debit card transactions does the **Applicant** process annually? _____

2. Does the **Applicant**:
   (a) Mask all but the last four digits of a card number when displaying or printing cardholder data? ☐ Yes ☐ No
   (b) Ensure that card-validation codes are not stored in any of the **Applicant's** databases, log files or anywhere else within their network? ☐ Yes ☐ No
   (c) Encrypt all account information on the **Applicant's** databases? ☐ Yes ☐ No
   (d) Encrypt or use tokenization for all account information at the point of sale? ☐ Yes ☐ No

Information Security Policies

1. Has the **Applicant** implemented a formal information security policy which is applicable to all of the **Applicant's** business units? ☐ Yes ☐ No

   If "Yes",
   (a) Does the **Applicant** test the security required by the security policy at least annually? ☐ Yes ☐ No
   (b) Does the **Applicant** regularly identify and assess new threats and adjust the security policy to address the new threats? ☐ Yes ☐ No
   (c) Does the **Applicant's** information security policy include policies for the use and storage of personally identifiable or other confidential information on laptops? ☐ Yes ☐ No

Web Server Security

1. Does the **Applicant** store personally identifiable or other confidential information on their web servers? ☐ Yes ☐ No
2. Do the **Applicant's** web servers have direct access to personally identifiable or other confidential information? ☐ Yes ☐ No
3. Does the **Applicant** have firewalls that filter both inbound and outbound traffic? ☐ Yes ☐ No

Virus Prevention, Intrusion Detection & Penetration Testing

1. Are anti-virus programs installed on all of the **Applicant's** PC's and network systems? ☐ Yes ☐ No

   If "Yes", how frequently are the virus detection signatures updated?

   _____

2. Does the **Applicant** employ intrusion detection or intrusion protection devices on their network, or IDS or IPS software on the **Applicant's** hosts? ☐ Yes ☐ No

   If "Yes", how frequently are logs reviewed? _____

3. Does the **Applicant** run penetration tests against all parts of their network? ☐ Yes ☐ No

   If "Yes", how often are the tests run? _____

4. Has the **Applicant** been the target of any computer or network attacks (including virus attacks) in the past 2 years? ☐ Yes ☐ No

   If "Yes", did the number of attacks increase? ☐ Yes ☐ No

Mobile Device Security

1. Does the **Applicant** store personally identifiable or other confidential information on mobile devices? ☐ Yes ☐ No

   If "Yes", does the **Applicant** encrypt such information? ☐ Yes ☐ No

Business Continuity

1. Does the **Applicant** have a Business Continuity Plan [BCP] specifically designed to address a network related denial-of-service attack? ☐ Yes ☐ No

   If "Yes":

   (a) Is the BCP reviewed and updated at least bi-annually? ☐ Yes ☐ No

   (b) Is the BCP tested at least annually? ☐ Yes ☐ No

   (c) Have any problems been rectified? ☐ Yes ☐ No

Security Assessments

1. Has an external system security assessment, other than vulnerability scans or penetration tests, been conducted within the past 12 months? ☐ Yes ☐ No

   If "Yes", please indicate who conducted the assessment, attach copies of the result, and indicate whether all critical recommendations been corrected or complied with. _____

   If "No", please attach explanation.

Backup & Archiving

1. How frequently does the **Applicant** back up electronic data? _____

2. Does the **Applicant** store back up electronic data with a third party service provider? ☐ Yes ☐ No

   If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? ☐ Yes ☐ No

   If "Yes" does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? ☐ Yes ☐ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? ☐ Yes ☐ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? ☐ Yes ☐ No

Service Providers

1. Does the **Applicant** use third-party technology service providers? ☐ Yes ☐ No

   If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? ☐ Yes ☐ No

If "Yes" does the **Applicant's** contract with the service provider(s) state that the service provider:

i) Has primary responsibility for the security of the **Applicant's** information? ☐ Yes ☐ No

ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? ☐ Yes ☐ No

iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? ☐ Yes ☐ No

Incident Response Plans

1. Does the **Applicant** have a formal incident response plan that addresses network security incidents or threats? ☐ Yes ☐ No

IV. SECURITY INCIDENT AND LOSS HISTORY:

1. Has the **Applicant** had any computer or network security incidents during the past two (2) years? "Incident" includes any unauthorized access or exceeding authorized access to any computer, system, data base or data; intrusion or attack; the denial of use of any computer or system; intentional disruption, corruption or destruction of electronic data, programs or applications; or any other incidents similar to the foregoing? ☐ Yes ☐ No

*Note: if the answer to Question 1 is "Yes", please attach a complete description of the incident(s), including whether the **Applicant** reported the incident(s) to law enforcement and/or the insurance carrier.*

V. ATTACHMENTS AND OTHER DOCUMENTS:

Please identify what additional documents are attached to, and/or submitted in conjunction with, this CyberSecurity New Business Application. All such documents are considered part of this CyberSecurity New Business Application.

☐ List of all organizations, in addition to the Parent Organization named in Section I, to be covered by this insurance;

(Note: If a policy is issued, only those organizations listed on this attachment will be Insureds, unless subject to the Newly Acquired Or Formed Organization condition.)

☐ CyberSecurity By Chubb[sm] Supplementary Questionnaire or ☐ CyberSecurity By Chubb[sm] Risk Matrix;

☐ Application from another insurance company for coverage that is similar to CyberSecurity By Chubb[sm];

☐ Risk assessment of the **Applicant** performed by an organization other than the **Applicant**;

☐ Other.

VI. WARRANTY: PRIOR KNOWLEDGE OF FACTS/CIRCUMSTANCES/SITUATIONS:

1 .The **Applicant** must complete the warranty statement below:

- For any **Liability** Coverage Part for which coverage is requested and is not currently purchased, as indicated in Section II, INSURANCE INFORMATION, Question 1 of this CyberSecurity New Business Application; or
- If the **Applicant** is requesting larger limits than are currently purchased, as indicated in Section II, INSURANCE INFORMATION, Question 1 of this CyberSecurity New Business Application.

The statement applies to those coverage types for which no coverage is currently maintained; and any larger limits of liability requested.

For Alaska, Florida, Maine, North Carolina and New Hampshire Residents ONLY: the title of this section and any other reference to "Warranty" is deleted and replaced with "**Applicant** Representation".

No person or entity proposed for coverage is aware of any fact, circumstance, or situation which he or she has reason to suppose might give rise to any claim that would fall within the scope of the proposed coverage:

NONE ☐ or, except

_____

_____

Without prejudice to any other rights and remedies of the Company, the **Applicant** understands and agrees that if any such fact, circumstance, or situation exists, whether or not disclosed in response to question 1 above, any claim or action arising from such fact, circumstance, or situation is excluded from coverage under the proposed policy, if issued by the Company.

VII. MATERIAL CHANGE:

If there is any material change in the answers to the questions in this CyberSecurity New Business Application before the policy inception date, the **Applicant** must immediately notify the Company in writing, and any outstanding quotation may be modified or withdrawn.

VIII. DECLARATIONS, FRAUD WARNINGS AND SIGNATURES:

The **Applicant's** submission of this CyberSecurity New Business Application does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the CyberSecurity New Business Application for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this CyberSecurity New Business Application.

The undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare that to the best of their knowledge and belief, after reasonable inquiry, the statements made in this CyberSecurity New Business Application and in any attachments or other documents submitted with this CyberSecurity New Business Application are true and complete. The undersigned agree that this CyberSecurity New Business Application and such attachments and other documents shall be the basis of the insurance policy should a policy providing the requested coverage be issued; that all such materials shall be deemed to be attached to and shall form a part of any such policy; and that the Company will have relied on all such materials in issuing any such policy.

The information requested in this CyberSecurity New Business Application is for underwriting purposes only and does not constitute notice to the Company under any policy of a Claim or potential Claim.

Notice to Arkansas, New Mexico and Ohio Applicants: Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

Notice to 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.

Notice to District of Columbia Applicants: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

Notice to 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.

Notice to Kentucky Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

Notice to Louisiana and Rhode Island 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 fines and confinement in prison.

Notice to 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.

Notice to Alabama and Maryland Applicants: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to New Jersey Applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to Oklahoma Applicants: Any person who, knowingly and with intent to injure, defraud or deceive any employer or employee, insurance company, or self-insured program, files a statement of claim containing any false or misleading information is guilty of a felony.

Notice to Oregon and Texas Applicants: Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

Notice to 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.

Notice to Puerto Rico Applicants: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Notice to 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.

Date	Signature*	Title
_____	_____	Chief Executive Officer
_____	_____	President

*****This CyberSecurity New Line Application must be signed by the Chief Executive Officer or President of the Parent Corporation acting as the authorized representatives of the person(s) and entity(ies) proposed for this insurance.

Produced By:

Agent: _____ Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

Submitted By:

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____