Chubb Group of Insurance Companies
15 Mountain View Rd.
Warren, NJ 07059

CYBERSECURITY BY CHUBB [SM]
SUPPLEMENTAL APPLICATION

BY COMPLETING THIS SUPPLEMENTAL CYBERSECURITY SUPPLEMENTAL APPLICATION THE APPLICANT IS APPLYING FOR COVERAGE WITH FEDERAL INSURANCE COMPANY (THE "COMPANY")

NOTICE: INSURING CLAUSE (A) OF THE CYBERSECURITY BY CHUBB[SM] POLICY PROVIDES CLAIMS-MADE COVERAGE, WHICH APPLIES ONLY TO "CLAIMS" FIRST MADE DURING THE "POLICY PERIOD", OR ANY APPLICABLE EXTENDED REPORTING PERIOD. THE LIMIT OF LIABILITY TO PAY DAMAGES OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY "DEFENSE COSTS", AND "DEFENSE COSTS" WILL BE APPLIED AGAINST THE RETENTION AMOUNT. IN NO EVENT WILL THE COMPANY BE LIABLE FOR "DEFENSE COSTS" OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF LIABILITY. READ THE ENTIRE CYBERSECURITY SUPPLEMENTAL APPLICATION CAREFULLY BEFORE SIGNING.

APPLICATION INSTRUCTIONS:

1. Whenever used in this CyberSecurity Supplemental Application, the term "**Applicant**" shall mean the Parent Organization and all subsidiaries, unless otherwise stated.

2. Include all requested underwriting information and attachments. Provide a complete response to all questions and attach additional pages if necessary.

3. In addition to the CyberSecurity New Line Application, the **Applicant** must complete the CyberSecurity Supplemental Application if the **Applicant** desires policy limits in excess of $5,000,000.

4. Please sign and date this Cyber Security Supplemental Application.

NAME OF **APPLICANT**: _____

I. GENERAL RISK INFORMATION:

Information Security Policies

1. Does the **Applicant's** information security policy identify and stipulate the types and levels of protection for all of the **Applicant's** information assets, whether electronic or otherwise, and whether held by the **Applicant** or by a person or organization providing services to the **Applicant**? ☐ Yes ☐ No
2. Which of the following elements are contained in the **Applicant's** information security policy? (Pick Multiple From Below)
   (a) Defined duties and responsibilities of an Information Security Officer. ☐ Yes ☐ No
   (b) Requirements for confidentiality agreements for employees, vendors and contractors. ☐ Yes ☐ No
   (c) Document classification, protection and destruction protocols. ☐ Yes ☐ No
   (d) Requirements for employee usage of system assets ☐ Yes ☐ No
   (e) Protection requirements for sensitive information stored on mobile devices (e.g. laptops, tablets, smartphones). ☐ Yes ☐ No
   (f) Protection requirements for sensitive information stored on other electronic media (e.g. backup tapes, CD's, USB drives). ☐ Yes ☐ No
3. Are all users of the **Applicant's** network issued unique passwords? ☐ Yes ☐ No
4. Do all users of the **Applicant's** network have designated rights and privileges for access to information and use of the **Applicant's** network? ☐ Yes ☐ No

5. Has the **Applicant** established policies for the following?

   (a) Internet usage ☐ Yes ☐ No

   (b) Acceptable use of social networking sites or applications ☐ Yes ☐ No

   (c) E-mail usage ☐ Yes ☐ No

   If "Yes" to any of the above in Question 5, do the **Applicant's** employees acknowledge that they are aware of each of the policies, or sections of the policies, that apply to them? ☐ Yes ☐ No

   If "No" to any of the above in Question 5, please explain:

   _____
   _____
   _____

6. Are the **Applicant's** information security and usage policies kept current and reviewed at least annually and updated as necessary? ☐ Yes ☐ No

Personnel Hiring Practices

1. Does the **Applicant's** management review the following for all prospective personnel who will have access to sensitive information?

   (a) Criminal history records ☐ Yes ☐ No

   (b) Credit history records ☐ Yes ☐ No

   (c) Records of previous employment ☐ Yes ☐ No

2. Do persons other than employees within the **Applicant's** organization, such as volunteers, interns or contract personnel, have access to sensitive information? ☐ Yes ☐ No

   If "Yes", are the same background checks (i.e. criminal, credit and previous employment) that are conducted on employees, also conducted on these persons? ☐ Yes ☐ No

Premises Security

1. Are all rooms (including "closets") that contain the **Applicant's** main frames, servers, switches and/or routers locked with access permitted with a key card or some other device that can be logged? ☐ Yes ☐ No

2. Does the **Applicant** investigate patterns of attempted access by persons who should not have access to equipment in Question 1, above? ☐ Yes ☐ No

3. Is the identity of all visitors (including vendors and repair personnel) verified prior to granting them access to any part of the **Applicant's** premises in which access to the **Applicant's** sensitive information or network can be attained? ☐ Yes ☐ No

Web Server Security

1. Does the **Applicant's** information security policy include all web-based systems? ☐ Yes ☐ No

2. Does the **Applicant** employ web application firewalls? ☐ Yes ☐ No

3. Are the **Applicant's** web servers housed in a dedicated DMZ? ☐ Yes ☐ No

4. Is all external access to sensitive information encrypted using SSL? ☐ Yes ☐ No

5. Does the **Applicant** have security policies governing the use of FTP, Telnet, Bash, etc.? ☐ Yes ☐ No

6. When are the **Applicant's** applications assessed for vulnerabilities such as SQL injection, cross-site scripting and buffer overflow? (Pick Multiple From Below)
   (a) During development? ☐ Yes ☐ No
   (b) At deployment to production? ☐ Yes ☐ No
   (c) Regularly after deployment? ☐ Yes ☐ No
7. How quickly does the **Applicant** remediate vulnerabilities after they are discovered? _____
8. Are user names and passwords sent in plain text over an insecure channel? ☐ Yes ☐ No
9. Does the **Applicant** restrict application privileges within the **Applicant's** databases to the minimum necessary levels? ☐ Yes ☐ No
10. Does the **Applicant** limit session lifetimes? ☐ Yes ☐ No
11. Does each application have its own set of permissions and access controls? ☐ Yes ☐ No
12. Have all unnecessary services and applications on each client and server been disabled? ☐ Yes ☐ No

Mobile Device Security

1. Is the **Applicant** alerted, or can the **Applicant** otherwise identify, when personally identifiable or other confidential information is:
   (a) Downloaded to a mobile memory device? ☐ Yes ☐ No
   (b) Sent in email, or added as an attachment to an email? ☐ Yes ☐ No
2. Does the **Applicant** encrypt data on smart phones? ☐ Yes ☐ No

Service Providers

1. For which of the following services does the **Applicant** utilize third-party service providers?
   (a) Back up of the **Applicant's** electronic data ☐ Yes ☐ No
   (b) Web site hosting ☐ Yes ☐ No
   (c) Processing or maintenance of sensitive data ☐ Yes ☐ No
   (d) Maintenance of applications ☐ Yes ☐ No
   (e) Infrastructure hosting ☐ Yes ☐ No
2. Has the **Applicant** evaluated the level of security provided by any of the service providers used, per the answers in Question 1, above? ☐ Yes ☐ No

   If "Yes", please indicate the method(s) by which their level of security was evaluated:
   (a) Review of SAS Type I ☐ Yes ☐ No
   (b) Review of SAS Type II ☐ Yes ☐ No
   (c) Review of security audit conducted by third party ☐ Yes ☐ No
   (d) **Applicant** conducted audit of **Applicant's** security ☐ Yes ☐ No
   (e) Other (Please provide a brief description): ☐ Yes ☐ No

   _____

PCI Compliance

1. Has a Qualified Security Assessor performed an assessment of the **Applicant's** security within the past year? ☐ Yes ☐ No

   If "Yes", who conducted the assessment? _____

   If "Yes", have all critical recommendations been corrected or complied with? ☐ Yes ☐ No

   If "No", when will all critical recommendations be corrected or complied with? _____

HIPAA Compliance

1. Is the **Applicant** a covered entity under the Health Insurance Portability and Accountability Act [HIPAA]? ☐ Yes ☐ No
2. Is the **Applicant** a Business Associate under the HIPAA? ☐ Yes ☐ No

If "Yes" to 1 or 2 above, approximately how many individuals' Protected Health Information do you collect, store or process? _____

If "Yes" to 1 or 2 above, is the **Applicant** in full or partial compliance with the provisions of the HITECH Act? ☐ Yes ☐ No

If the **Applicant** is in partial compliance with the HITECH Act, when will the **Applicant** be in full compliance? _____

3. Has the **Applicant** been audited by The Department of Health and Human Services [HHS}, or any other agency under the authority of HHS, for their compliance with the HIPAA Privacy Rule and/or Security Rule? ☐ Yes ☐ No

   If "Yes", was the **Applicant** found to be in compliance? ☐ Yes ☐ No

   If "No", please indicate in which areas the **Applicant** was found not to be in compliance:

   _____

   _____

   _____

   Have all areas of non compliance been rectified? ☐ Yes ☐ No

4. Does the **Applicant** conduct regular audits of their HIPAA Privacy and Security controls and procedures? ☐ Yes ☐ No
5. Does the **Applicant** remediate any areas in which they are found not to be in compliance within:

   (a) 30 days; ☐ Yes ☐ No

   (b) 90 days; ☐ Yes ☐ No

   (c) 180 days; ☐ Yes ☐ No

   (d) more than 180 days. ☐ Yes ☐ No

6. In the **Applicant's** contracts with any of their Business Associates does the **Applicant** require that the business associates indemnify the **Applicant** for any liability the **Applicant** incurs as a result of the business associates' non-compliance with HIPAA, the Hi Tech Act or any failure or alleged failure to keep the **Applicant's** information secure? ☐ Yes ☐ No

Written Records Management

1. Does the **Applicant** collect sensitive information through hand written applications, forms or notes? ☐ Yes ☐ No

   If "Yes", does the **Applicant** shred such documents after entering the information into their computer system? ☐ Yes ☐ No

   If "No", does the **Applicant**:

   (a) Retain the documents in secured files? ☐ Yes ☐ No

   (b) Store such documents in secure areas that minimize access by persons not authorized to view such documents? ☐ Yes ☐ No

   (c) Enforce a clean desk policy? ☐ Yes ☐ No

   (d) Shred such documents when they are ultimately disposed of? ☐ Yes ☐ No

2. Is sensitive information in *any written form* (handwritten, typed, or printed) stored with a third party? ☐ 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:

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

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

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

Data Breach Incident Response

*Please complete this Section if the **Applicant** answered "Yes" to Question 1(a) in the Incident Response Plan Section of the CyberSecurity By Chubb[SM] New Business Application, indicating that they have a formal, written incident response plan that addresses unauthorized access to the **Applicant's** computers, system, network or any of their information assets.*

1. Does the **Applicant's** Incident Response Plan address the following network security incidents or threats:

   (a) Unauthorized access to the **Applicant's** computers, system, network, or any of the **Applicant's** information assets? ☐ Yes ☐ No

   (b) Known or suspected unauthorized access to personally identifiable or other confidential information? ☐ Yes ☐ No

   (c) Denial of service attacks and other forms of network or system outages? ☐ Yes ☐ No

   (d) Extortion demands? ☐ Yes ☐ No

   (e) Corruption of, or damage to, electronic data? ☐ Yes ☐ No

   If "Yes" to any of the above in Question 1,

   i) Has the plan been reviewed and approved by the **Applicant's** board of directors (or persons with substantially similar responsibilities)? ☐ Yes ☐ No

   ii) Does the incident response plan include a review of applicable state or federal laws or regulations or other standards with which the **Applicant** may have to comply? ☐ Yes ☐ No

iii) Does the **Applicant** test the security incident response plan at least annually and address any issues identified in the tests? ☐ Yes ☐ No

iv) Has the **Applicant** estimated the financial cost to respond to an incident of unauthorized access to personally identifiable or other confidential information (i.e. data breach)? ☐ Yes ☐ No

If "Yes", what is the estimated cost? _____

v) Is a specific person or group of persons responsible for maintaining the IRP? ☐ Yes ☐ No

vi) How often is the **Applicant's** IRP updated? _____

2. Does the Incident Response Plan identify:

(a) The law firm(s) or other organization(s) that will determine the applicability of state or federal laws? ☐ Yes ☐ No

(b) The organization(s) that will provide mailing or other notification services? ☐ Yes ☐ No

(c) The organization(s) that will provide public relations services? ☐ Yes ☐ No

(d) The organization(s) that will provide credit or other monitoring services? ☐ Yes ☐ No

(e) The organization(s) that will provide forensic services? ☐ Yes ☐ No

II. 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 the 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 the 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.

III. MATERIAL CHANGE:

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

IV. DECLARATIONS, FRAUD WARNINGS AND SIGNATURES:

The **Applicant's** submission of this CyberSecurity Supplemental Application does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the CyberSecurity Supplemental Application for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this CyberSecurity Supplemental 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 Supplemental Application and in any attachments or other documents submitted with this CyberSecurity Supplemental Application are true and complete. The undersigned agree that this CyberSecurity Supplemental 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 Supplemental 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 Maryland Applicants: Any person who knowingly and willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly and 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 Supplemental 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: _____