



Chubb Cyber Enterprise Risk Management Policy<sup>SM</sup>  
Coverage Application

Please read carefully. Fully answer all questions and submit all requested information for each Coverage you seek. Provide any supporting information on separate sheets, attached to this Application, using your letterhead and reference the applicable question numbers. All such separate sheets shall be deemed attached to, incorporated into, and become part of this Application. All applicants must complete the General Information and Declaration and Certification sections of this Application. Underwriters will rely upon all statements made in this Application and attachments.

**I. GENERAL INFORMATION (Required of all applicants):**

- 1. Name of Educational Institution: \_\_\_\_\_  
(hereinafter, "Educational Institution", "Applicant," "you," or "your")  
Mailing Address: \_\_\_\_\_  
\_\_\_\_\_
- 2. Web address(es): \_\_\_\_\_
- 3. Nature of Educational Institution's Internet Activities:  
\_\_\_\_\_  
\_\_\_\_\_

**II. EDUCATIONAL INSTITUTION STATISTICS, INTERNET ACTIVITIES and CONTROLS (Required of all applicants):**

Year Established: \_\_\_\_\_ Projected Annual Budget (Current if projected budget is unavailable): \_\_\_\_\_  
 Number of Employees (Teachers/Volunteers/Other): \_\_\_\_\_ Number of Students: \_\_\_\_\_  
 Number of unique hits to website(s) annually: \_\_\_\_\_ Percentage of Revenue from e-commerce activity: \_\_\_\_\_%

- Does the Applicant provide technology services or products to third parties? Yes No
- Do third parties rely on the availability of the Applicant's web site(s) in order to transact business? Yes No

**INFORMATION MANAGEMENT:**

- 1. Has legal counsel checked that your domain name(s) and metatags do not infringe on another's trademark? Yes No
- 2. Does the educational institution have a written and posted privacy policy on your site(s)? Yes No

**INFORMATION SECURITY:**

- 1. Does the Applicant have procedures in place to ensure compliance with privacy legislation (such as the Health Insurance Portability and Accountability—HIPAA, the Gramm-Leach-Bliley Act or other applicable legislation) with respect to the protection of confidential information? Yes No  
If in process and not completed please provide percentage completed to date: \_\_\_\_\_%
- 2. Does the Applicant store sensitive, personal, or confidential information on web servers? Yes No  
If so, is this information located behind a firewall? Yes No
- 3. Does your educational institution sell or share individual subscriber or user identifiable information with other internal or external entities? Yes No

- |   |     |    |
|---|-----|----|
| 4. Have you ensured that all sensitive business/consumer information that is transmitted within your educational institution or to/from other public networks has been encrypted using industry-grade mechanisms?   | Yes | No |
| 5. Have you also ensured that all sensitive business/consumer information that resides within your educational institution's systems has been encrypted while "at-rest" within databases or other electronic data files?  | Yes | No |
| 6. Have you ensured that all sensitive business/consumer information that is physically transmitted via tape or any other medium – between your educational institution's facilities and those of your business partners/service providers has been encrypted?  | Yes | No |
| 7. For computer equipment that leaves your physical facilities (e.g., mobile laptops, PDAs, smartphones, and home-based desktops), have you implemented strong access control requirements and hard drive encryption to prevent unauthorized exposure of company data in the event these devices are stolen, lost or otherwise unaccounted for? | Yes | No |
| 8. Does your educational institution follow established procedures for carrying out and confirming the destruction of paper files and data residing on systems or devices prior to their recycling, refurbishing, resale, or physical disposal?   | Yes | No |
| 9. Does your educational institution employ a chief privacy officer (or equivalent) who has enterprise-wide responsibility for meeting the obligations under the jurisdictional privacy and data protection laws that apply to the educational institution?   | Yes | No |
| 10. Has your educational institution – in response to Pennsylvania law - established a proactive procedure for determining the severity of potential data security breaches and providing prompt notification to all individuals who may be adversely affected by such exposures?   | Yes | No |
| 11. Has your educational institution implemented procedures for honoring the specific marketing "opt- out" requests of your customers that are fully consistent with the terms of your currently published privacy policy?  | Yes | No |
| 12. Does your educational institution conduct regular reviews of your third-party service providers and partners to ensure that they adhere to your contractual requirements for the protection of sensitive business/customer data that you entrust to their care for processing, handling, and marketing purposes?                            | Yes | No |
| 13. Do contracts with third-party service providers include indemnity provisions that protect you from any liability arising out of their loss of your sensitive information?   | Yes | No |
| 14. Does the Applicant maintain an information systems security policy, including laptop security policy?   | Yes | No |
| 15. Does the Applicant have a computer security breach Incident Response Plan (IRP)?  | Yes | No |
| 16. Has the Applicant had an external system security assessment and/or a network penetration test conducted within the last 12 months?   | Yes | No |
| If so, have all critical recommendations been addressed and resolved?   | Yes | No |

**CYBER CRIME:**

- |   |     |    |
|---|-----|----|
| 1. Does the Applicant accept funds transfer information from clients over the telephone, email, text message or similar method of communication?        | Yes | No |
| 2. Does the Applicant authenticate instructions by calling the customer at a predetermined phone number or require receipt of a customer identity code? | Yes | No |
| 3. Is approval by more than one person required to initiate a wire transfer?  | Yes | No |



Chubb Cyber Enterprise Risk Management Policy<sup>SM</sup>  
Coverage Application

- 4. Does the Applicant verify all vendor and supplier bank accounts by a direct call to the receiving bank, prior to accounts being established in the accounts payable system? Yes No

**CLAIMS EXPERIENCE:**

- 1. Has the Applicant had any computer security incidents, any allegations that personal information was compromised, and/or notified customers that their information was or may have been compromised during the past five (5) years (incident refers to any unauthorized access, intrusion, breach, compromise or use of the Applicant's computer systems, including theft of money, proprietary information, or confidential customer information, denial of service, electronic vandalism or sabotage, computer virus or other computer incidents)? Yes No
- 2. Is the Educational Institution or any of its partners, principals, directors or officers aware of, or are there any circumstances that may give, or have given, rise to a claim against the company or against this insurance policy? Yes No
- 3. In the last five years has the Educational Institution experienced any claims or are you aware of any circumstances that could give rise to a claim that would be covered by the this policy? Yes No
- 4. Within the past three years, has the Applicant had any actual or potential Funds Transfer Fraud, Computer Fraud, or Social Engineering Fraud Incidents or Claims? Yes No
- 5. Is the Applicant aware of any notices, facts, circumstances or situations that could reasonably be expected to give rise to a Funds Transfer Fraud, Computer Fraud, or Social Engineering Fraud Incident or Claim? Yes No

If yes to any question above, please provide details.

It is understood and agreed that if any such incident, allegation, or notification exists or occurred (whether or not reported above), then: (i) such incident, allegation and notification; and (ii) any Claim arising from any such incident, allegation, or notification, are excluded from coverage under the Policy.

**IV. FRAUD NOTICE**

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

**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.

**V. MATERIAL CHANGE**

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

**VI. DECLARATION AND SIGNATURE**

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



Chubb Cyber Enterprise Risk Management Policy<sup>SM</sup>  
Coverage Application

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

This Application must be signed by the risk manager or a senior officer of the Parent Organization, acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Signature of Authorized Applicant:

\_\_\_\_\_

Print Name

\_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Signature of Broker/Agent:

\_\_\_\_\_

Print Name

\_\_\_\_\_

Date: \_\_\_\_\_

Signed by Licensed Resident Agent

\_\_\_\_\_

(Where Required By Law)

