The Hartford Steam Boiler Inspection and Insurance Company
One State Street
Hartford, Connecticut 06102

HSB TOTAL CYBER™
CYBER RISK INSURANCE APPLICATION

INSURANCE UNDERWRITTEN BY THE HARTFORD STEAM BOILER INSPECTION AND INSURANCE COMPANY

NOTICES

- The cyber risk coverage part provides that the limit of liability available to pay judgments or settlements shall be reduced and may be exhausted by amounts incurred for legal defense. Further note that amounts incurred for legal defense shall be applied against the deductible amount.
- If a cyber risk coverage part is issued, it will be on a claims-made and reported basis. Please read the entire cyber risk coverage part carefully to determine rights, duties and what is and is not covered.

SECTION I – COVERAGE REQUESTED

Proposed Policy Effective Date:

LIMIT OF LIABILITY REQUESTED

$50,000 **$100,000** **$250,000** **$500,000** **$1,000,000** **$2,000,000** **$3,000,000** **$5,000,000** **$10,000,000**

SECTION II – GENERAL INFORMATION

POLICY PERIOD REQUESTED:
From: **To:**

APPLICANT NAME AND ALL SUBSIDIARIES

APPLICANT ADDRESS *(Corporate Headquarters)*	CITY	STATE	ZIP CODE

APPLICANT MAILING ADDRESS *(If different from above)*	CITY	STATE	ZIP CODE

GROSS REVENUES: Projected Year	**NET OPERATING EXPENSES:** *(Education and Public Administration Only)* Projected Year	**GROSS REVENUES:** From Goods or Services to Customers via the Internet

DATE BUSINESS ESTABLISHED	NUMBER OF EMPLOYEES	BUSINESS DESCRIPTION

LIST ALL WEBSITE URL'S.

STOP No additional information necessary if limit requested does **not** exceed $500,000. Otherwise, please proceed.

SECTION III – GENERAL UNDERWRITING QUESTIONS AND LOSS INFORMATION

	YES	NO	N/A
1. Do you encrypt all your mobile devices *(laptops, flash drives, mobile phones, etc.)* and confidential data?	☐	☐	
2. Do you use up-to-date anti-virus and anti-malware protection on all of your endpoints (*desktops, laptops, servers, etc.*) and firewalls on all of your internal access points?	☐	☐	
3. Do you restrict employees' and external users' IT systems privileges and access to personal information on a business-need-to-know basis?	☐	☐	
4. Do you perform backups of business critical data on at least a weekly basis?	☐	☐	
5. Have you, at any time during the past 36 months, experienced a cyber incident *(hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.)* that cost you more than $10,000 or experienced a lawsuit or other formal dispute *(with either a private party or government agency)* arising from a cyber incident?	☐	☐	

SECTION III – GENERAL UNDERWRITING QUESTIONS AND LOSS INFORMATION - *continued*

	YES	NO	N/A
6. Within the past 12 months, did you or one of your cloud providers experience an unplanned outage lasting longer than 2 hours? *(This does not include failure caused by an unauthorized access ("cyber attack")).* If **"Yes",** please attach details.	☐	☐	

No additional information necessary if limit requested does **not** exceed $1,000,000. Please sign and date application. Otherwise, please proceed.

SECTION IV – DEVICES, INFORMATION AND VENDOR MANAGEMENT

1. How many of the following devices to you currently have deployed?

- Servers: .....
- Desktops: .....
- Laptops: .....
- Mobile Phones/ Devices: .....

2. How many individual people *(employees, customers, etc.)* do you currently store or maintain *(either yourself or using third parties)* information about?

.....

	YES	NO	N/A
3. Do you process or store personal information or other confidential information for other businesses or organizations?	☐	☐	
4. For each vendor that processes or stores personal information for you, do you have a written agreement that makes the vendor financially responsible for the consequences of a cyber attack or data breach? *(If you do not engage any such vendors, answer **"Yes"**)*	☐	☐	
5. Do you require service providers to demonstrate adequate security?	☐	☐	

SECTION V – INTERNAL POLICIES, COMPLIANCE AND PRIVACY MANAGEMENT

1. Do you have a written organization-wide privacy and security policy?	☐	☐	
2. Do you have a document retention and destruction policy?	☐	☐	
3. Have you implemented a *written* policy requiring:			
a) telephone confirmation *(or by means other than email)* with the payee or requestor, of the payment details before making payments *(including wire and ACH transfers*) in excess of $10,000?	☐	☐	
b) multiple internal parties to confirm authorization before making payments *(including wire and ACH transfers)* in excess of $10,000?	☐	☐	
4. Does each user of your system have a separate individual account?	☐	☐	
5. Do you have a formal process *(which includes identification, tracking, and monitoring)* in place for properly bringing servers, desktops, laptops and other digital assets into service and a formal process *(which includes removal from the network, deleting from inventory and secure wiping of sensitive data)* for properly removing those assets from service?	☐	☐	
6. If you accept payment *(credit and debit)* cards, do you comply with Payment Card Industry Data Security Standards? *(If you do not accept payment cards, answer **"N/A"**)*	☐	☐	☐
7. If you handle health information, do you comply with HIPAA and the HITECH act? *(If you do not handle health information, answer **"Yes"**)*	☐	☐	
8. Do you have a designated Chief Information Officer or other person responsible for information and systems security?	☐	☐	
9. Have you identified and secured personal and other highly confidential information for which you are responsible?	☐	☐	

SECTION VI – NETWORK SECURITY AND INCIDENT MANAGEMENT

	YES	NO	N/A
1. Do you update and patch critical IT-systems and applications on at least a monthly basis?	☐	☐	
2. Have you implemented the use of long and complex passwords or another secure account-access methodology such as multifactor identification or universal identification?	☐	☐	

SECTION VI – NETWORK SECURITY AND INCIDENT MANAGEMENT - *continued*

	YES	NO	N/A
3. Are all Internet-accessible systems *(for example, web-, email-servers)* segregated *(for example, within a DMZ or at a 3rd party provider)* from your trusted network?	☐	☐	
4. Do you use intrusion detection hardware or software or otherwise monitor your network and identify security events?	☐	☐	
5. Do you provide awareness training for employees in data privacy and security issues *(including legal liability issues and phishing)*?	☐	☐	
6. Do you delete system access, accounts and associated rights after termination of users *(including employees, temporary employees, contractors and vendors*)?	☐	☐	
7. Do you *(yourself or by engaging an outside vendor)* regularly scan critical systems for security vulnerabilities? These scans may include security and penetration testing.	☐	☐	
8. If you perform backups of business critical data on at least a weekly basis, is the backup stored offsite in a secure location? *(If you do not backup business critical data on at least a weekly basis, answer **"N/A"**)*	☐	☐	☐
9. If you perform backups of business critical data on at least a weekly basis, do you test your restore process on at least a monthly basis? *(If you do not backup business critical data on at least a weekly basis, answer **"N/A"**)*	☐	☐	☐
10. Do you have a business continuity management or disaster recovery plan in place?	☐	☐	
11. Do you have an incident response plan *(for cyber attacks and data breaches)* that identifies an incident response team?	☐	☐	
12. Do you have a process in place to review all advertising and other content prior to publication?	☐	☐	

FRAUD WARNINGS

NOTICE TO APPLICANTS IN STATES NOT SPECIFICALLY ADDRESSED BELOW:
Any person who knowingly, and with intent to defraud or deceive 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 act, which is a crime and may subject such person to criminal and civil penalties.

NOTICE TO ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, LOUISIANA, MARYLAND, NEW MEXICO, RHODE ISLAND AND WEST VIRGINIA APPLICANTS:
Any person who knowingly (or willfully in MD) presents a false or fraudulent claim for payment of a loss or benefit or knowingly (or willfully in MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison, or any combination thereof.

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 policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claiming with regard to a settlement or award payable for insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

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 KANSAS APPLICANTS:
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.

NOTICE TO KENTUCKY, NEW YORK 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.

NOTICE TO MAINE, 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 denial of insurance benefits.

NOTICE TO NEW HAMPSHIRE APPLICANTS:
Any person who, with a purpose to injure, defraud or deceive any insurance company, files a statement of claim containing any false, incomplete or misleading information is subject to prosecution and punishment for insurance fraud as provided in RSA 638.20.

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:
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.

NOTICE TO OREGON 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 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. If 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.

*Please **read** the following statement **carefully** and **sign** where indicated.*

The undersigned authorized officer, owner or manager of the Applicant hereby acknowledges that he/she is aware that the limit of liability contained in the Cyber Coverage Part shall be reduced, and may be completely exhausted, by the costs of legal defense and, in such event, the insurer shall not be liable for the costs of legal defense or for the amount of any judgment or settlement to the extent that such exceeds the limit of liability of the Cyber Coverage Part.

The undersigned authorized officer, owner or manager of the Applicant hereby acknowledges that he/she is aware that legal defense costs that are incurred shall be applied against the deductible amount.

The undersigned authorized officer, owner or manager of the applicant declares that the information furnished in this application is complete, true and correct. The undersigned authorized officer, owner or manager 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.

Any intentional or negligent misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for the rescission** of any bond or policy issued.

** For **Maine and Maryland** Applicants **ONLY**: The word “rescission” is deleted and replaced with “denial”.

For **Georgia** Applicants **ONLY**:
Any misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for denying coverage and cancelling any bond or policy issued.

For **Louisiana** Applicants **ONLY**:
Any misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for the denial of any claim related to any such misrepresentation, omission, concealment or incorrect statement or the cancellation of any bond or policy issued, provided that coverage will continue for legitimate claims until the cancellation is effective.

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 cyber coverage part be issued.

AUTHORIZATION

Applicant Signature: .....
(Must be signed by Officer, Owner or Manager)

Printed Name: .....

Title: .....

Date: .....

Producer: .....

Producer's Address: .....

Producer's Signature: .....

Date: .....

License Number: .....

Please return this completed form to: HSBTotalCyber@hsb.com