

New Business Application

CLAIMS-MADE NOTICE

THIS IS AN APPLICATION FOR COVERAGE WHICH IS PROVIDED ON A CLAIMS-MADE BASIS; THEREFORE, THIS POLICY PROVIDES NO COVERAGE FOR CLAIMS ARISING OUT OF WRONGFUL ACTS WHICH TOOK PLACE PRIOR TO THE RETROACTIVE DATE STATED IN THE POLICY. SUBJECT TO ITS TERMS, THIS POLICY WILL APPLY ONLY TO CLAIMS ACTUALLY MADE OR INCIDENTS REPORTED AGAINST YOU WHILE THE POLICY REMAINS IN EFFECT. ALL COVERAGE UNDER THIS POLICY CEASES UPON TERMINATION OF THIS POLICY EXCEPT FOR THE AUTOMATIC EXTENDED REPORTING PERIOD OF 60 DAYS OR AN EXTENDED REPORTING PERIOD OF 12, 24 OR 36 MONTHS THAT YOU MAY CHOOSE TO PURCHASE. POTENTIAL GAPS MAY ARISE UPON EXPIRATION OF THE EXTENDED REPORTING PERIODS. DURING THE FIRST SEVERAL YEARS OF THE CLAIMS-MADE RELATIONSHIP, CLAIMS-MADE RATES ARE COMPARATIVELY LOWER THAN OCCURRENCE RATES. YOU CAN EXPECT SUBSTANTIAL ANNUAL PREMIUM INCREASES, INDEPENDENT OF OVERALL RATE LEVEL INCREASES, UNTIL THE CLAIMS-MADE RELATIONSHIP REACHES MATURITY.

CLAIM EXPENSES WITHIN LIMITS

This Policy will be written on a claim expenses within limits basis. The Limit of Liability can be completely exhausted by claim expenses and we have no liability for legal defense costs or for the amount of any judgment or settlement in excess of the limits stated in your policy. claim expenses will be applied against the retention. Please read and review your policy carefully.

INSTRUCTIONS

Whenever used in this **Application**, the term **Applicant** shall mean the **Named Insured** and all **Subsidiaries** or other organizations applying for coverage, unless otherwise stated.

I. GENERAL INFORMATION

Name of **Applicant**: _____

Address of **Applicant**: _____

City: _____ State: _____ Zip Code: _____ Year Established: _____

NOTICE: THESE POLICY FORMS AND THE APPLICABLE RATES ARE EXEMPT FROM THE FILING REQUIREMENTS OF THE NEW YORK INSURANCE LAW AND REGULATIONS. HOWEVER, SUCH FORMS AND RATES MUST MEET THE MINIMUM STANDARDS OF THE NEW YORK INSURANCE LAW AND REGULATIONS.

Total number of **Employees** (full and part time): _____ **Applicant's URL:** _____

Applicant's NAICS code: _____ **Applicant's Annual Revenue:** \$ _____

% revenue derived from Government contracts: _____ % **Description of Applicant's Operations:** _____

Does the **Applicant** have any physical offices, operations or **Subsidiaries** outside of the United States? Yes No

Does the **Applicant** have any sales outside of the United States? Yes No If "Yes", amount: \$ _____

Indicate the total (estimated) number of the unique records collected/maintained by the **Applicant**:

<50,000 50k-500k 500k-1M >1M-3M >3M Estimated Number of *annual* Credit Card Transactions if applicable: _____

Indicate the nature of the **Data**:

Biometric Information Corporate Sensitive Financial Account Numbers Other Personally Identifying Information (i.e. SSNs & passport #'s) Protected Health Information Other information (i.e. name, address, phone number, etc.)

II. REQUESTED COVERAGES

Indicate below which coverages are being requested:

Requested Coverage	Requested Limit(s)	Requested Retentions	Requested Retro Date
Third Party Liability Coverage			
<input type="checkbox"/> Privacy and Security Liability	\$	\$	
<input type="checkbox"/> Media and Content Liability	\$	\$	
<input type="checkbox"/> Fines, Penalties and Regulatory Defense	\$	\$	

Requested Coverage	Requested Limit(s)	Requested Retentions
First Party Expense Coverage – Response Costs		
<input type="checkbox"/> Security Breach Notification and Remediation	\$	\$
<input type="checkbox"/> Systems Restoration	\$	\$
<input type="checkbox"/> Cyber Extortion	\$	\$
<input type="checkbox"/> Public Relations	\$	\$
<input type="checkbox"/> Cyber Breach or Extortion Reward	\$	\$
<input type="checkbox"/> Hardware Replacement Expense	\$	\$
<input type="checkbox"/> Payment Card Expense	\$	\$
First Party Expense Coverage – Loss of Income		
<input type="checkbox"/> Business Income Loss and Extra Expense	\$	Hrs.
<input type="checkbox"/> Contingent Business Income Loss and Extra Expense	\$	Hrs.
<input type="checkbox"/> Reputational Harm Expense	\$	\$
First Party Expense Coverage – Fraud Loss		
<input type="checkbox"/> Funds Transfer Fraud	\$	\$
<input type="checkbox"/> Computer Fraud	\$	\$
<input type="checkbox"/> Systems Resource Fraud	\$	\$
<input type="checkbox"/> Social Engineering	\$	\$
Supplemental Coverage		
<input type="checkbox"/> Court Attendance Costs	\$	Not Applicable

III. PRIVACY AND SECURITY

1. The **Applicant** has (check all that apply):
 - a. A regularly tested and updated Written Information Security Plan
 - b. A regularly tested and updated Written Incident Response Plan
 - c. A designated Chief Information Security Officer (or equivalent)
2. Back-ups – The **Applicant** makes (*select one*):
 - a. Regular, full and incremental backups of critical **Data** and **Computer Systems**
 - b. Occasional and full back-ups of critical **Data** and **Computer Systems**
 - c. No back-ups of critical **Data** and **Computer Systems**

If either 2.a. or 2.b. has been selected is one copy stored on-line? Yes No

If either 2.a. or 2.b. has been selected is one copy stored off-site and *off-line*? Yes No

If either 2.a. or 2.b. has been selected how quickly could systems be operational:

Within 24 hours Within 25-48 hours Within 49-130 hours Greater than 130 hours
3. Background checks – For **Employees** with access to sensitive data & systems, the **Applicant** conducts (*select one*):
 - a. Full, nationwide, criminal background, sex offender, and credit checks
 - b. Full, nationwide, criminal background checks
 - c. No background checks
4. Patching & Updates – The **Applicant** has (*select one*):
 - a. Automatic updates enabled with patch management verification procedure
 - b. Automatic updates enabled
 - c. Manual updates
5. Information Security Training – The **Applicant** has the following employee training program to safeguard **Personal Information** (*select one*):
 - a. Formal and documented *annual* **Employee** training program
 - b. Formal but undocumented **Employee** training program
 - c. No **Employee** training program
6. Firewalls – The **Applicant** has (*select one*):
 - a. **Hardware** and software firewalls deployed
 - b. **Hardware** firewall deployed
 - c. No firewalls deployed
7. Endpoint Detections & Response (EDR) and Intrusion Detection Software – The **Applicant** has (*select one*):
 - a. EDR and Intrusion detection software installed or activated on all **Computer Systems**
 - b. EDR solution installed or activated on all endpoints
 - c. No EDR solution or intrusion detection software installed or activated
8. Network Security – When working remotely, the **Applicant's Employees** (*select one*):
 - a. Access a segmented network via Virtual Private Network with Multi-Factor Authentication
 - b. Access a segmented network via Virtual Private Network
 - c. Do not access a Virtual Private Network
9. Email Security – The **Applicant** has (*select one*):
 - a. Web and email (DKIM, DMARC, SPF) filtering enabled
 - b. Web or email (DKIM, DMARC, SPF) filtering enabled
 - c. Neither web nor email filtering enabled

10. Encryption – Encryption is (*select one*):
- a. Deployed for **Data** at rest, in transit and on mobile devices
 - b. Deployed for **Data** at rest
 - c. Not deployed - Please Explain: _____
11. Accountability - When accessing **Computer Systems** & information, **Employees** & 3rd parties are issued (*select one*):
- a. Separate & unique accounts with strong passwords (e.g. NIST, MS, etc.) and Multi-Factor Authentication deployed; Access is restricted to that needed to perform their duties, e.g. separate administration accounts.
 - b. Separate & unique accounts with strong passwords (e.g. NIST, MS, etc.)
 - c. Separate & unique accounts with no password construction requirements
12. **Data** Destruction – When **Data** and equipment is no longer needed, the **Applicant** (*select one*):
- a. Disposes **Hardware**/media responsibly in accordance with a written **Data** retention & destruction policy
 - b. Disposes of old computers/devices/media responsibly
 - c. Has no policies or procedures pertaining to the destruction of **Data** or retirement of **Hardware**
13. Has traffic using Remote Desktop Protocol (RDP) TCP ports 3389 and Server Message Block (SMB) TCP ports 445, 135, and 139 been blocked? Yes No

IV. MEDIA LIABILITY

1. Does the **Applicant** have the following procedures with respect to **Your** website:
- a. All content is reviewed prior to being posted on the **Applicant's** website to avoid improper, offensive or infringing content including intellectual property, trademarks and service marks? Yes No
 - b. If user information is collected, the user has the option to opt-in or opt-out of allowing the collection or use of their information? Yes No
 - c. If **Personal Information** gathered from customers is sold, the **Applicant** notifies and obtains consent prior to dissemination of such information? Yes No
2. Does the **Applicant** consistently monitor & remove offensive, unacceptable or infringing posts from **Your** website or Social Media site? Yes No
- Please note any explanations to any "No" answers for Questions 1 and 2 here: _____
- _____

V. SOCIAL ENGINEERING / PHISHING

1. Does the **Applicant** have written and documented procedures in place which are provided to **Your Employees** and which require **Employees** to authenticate all requested changes to vendor/supplier Or client/customer information (such as changes to bank accounts, routing numbers, contact information) with a phone call to an authorized representative of the vendor/supplier or client/customer at a pre-determined phone number on file? Yes No
- If "No", please explain your procedures for authenticating an internal wire transfer request.
- _____
2. Does the **Applicant** have written and documented procedures which are provided to **Your Employees**, whereby **Your Employees** that process wire transfers are to never process an owner/Sr. Exec/**Employee** directed request wire transfer without first validating the request with a call back to the requestor (inclusive of any owner) at a pre-determined work phone number or with a face to face confirmation? Yes No
- If "No", please explain your procedures for authenticating an internal wire transfer request.
- _____

3. Does the **Applicant** provide social engineering/phishing training on at least an annual basis to **Employees** that have wire transfer or accounts payable authority that educates **Employees** on how to:
- Detect and identify social engineering/phishing scams where a fraudulent email or phone call from purported vendor or client is received, requesting their vendor or client bank account information be changed? Yes No
 - Detect and identify social engineering/phishing scams where a fraudulent email or phone call from a purported owner or employee of the **Applicant** is received, requesting a wire transfer be made on their behalf? Yes No
- If "No", what kind of training does the **Applicant** provide to help combat these types of fraudulent schemes and how often?
-

VI. PRIOR LOSS AND KNOWLEDGE INFORMATION

Note: Please attach additional pages when listing any events below, separately note each event including dates, description, amounts of loss, and corrective measures.

Within the past 3 years has the **Applicant**:

- Notified consumers or any third party of a data breach incident? Yes No
- Experienced an actual or attempted extortion demand with respect to **Your Computer System**? Yes No
- Experienced an unscheduled network outage lasting over 4 hours? Yes No
- Received a complaint or cease and desist demand alleging trademark, copyright, invasion of privacy, or defamation with regards to any content published, displayed or distributed by or on behalf of the **Applicant**? Yes No

Is any **Applicant** proposed for coverage aware of any fact, circumstance, or situation that might reasonably be expected to result in a **Claim** that would fall within the scope of the proposed coverage? Yes No

If "Yes" please attach a full description of the details.

VII. MATERIAL CHANGE

If any of the **Applicants** discover or become aware of any significant change in the condition of the **Applicant** between the date of this **Application** and the Policy inception date, which would render the **Application** inaccurate or incomplete, notice of such change will be reported in writing to us immediately and any outstanding quotation may be modified or withdrawn.

VIII. DECLARATIONS, NOTICE AND SIGNATURES

The authorized signer of this **Application** represents to the best of his/her knowledge and belief that the statements set forth herein are true, accurate, complete and include all material information. The authorized signer also represents that any fact, circumstance or situation indicating the probability of a **Claim** or legal action now known to any entity, official or employee involving the proposed coverage has been declared, and it is agreed by all concerned that the omission of such information shall exclude any such **Claim** or action from coverage under the insurance being applied for, whether or not disclosed. Any **Claim** based upon, arising out of or in connection with any misrepresentation, omission, concealment, untruthful, inaccurate, or incomplete statement of a material fact in this supplemental **Application** or otherwise shall be excluded from coverage. Signing of this **Application** does not bind The Hanover Insurance Company or any of its insurance affiliates or subsidiaries to offer, nor the authorized signer to accept insurance. It is agreed this **Application** and any attachments hereto shall be the basis of the insurance and will be incorporated by reference and made part of the Policy should a Policy be issued.

ATTENTION APPLICANTS

NEW YORK: 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 civil penalties not to exceed five thousand dollars and the stated value of the claim for each such violation.

SIGNATURE OF APPLICANT'S AUTHORIZED REPRESENTATIVE

Date

Signature**

Title

**This New Business Application must be signed by the chief executive officer, president, or chief financial officer of the Applicant's parent organization acting as the authorized representatives of the person(s) and entity(ies) proposed for this insurance.

Produced By: Producer: _____ Agency: _____

Taxpayer ID: _____ License Number: _____ Email: _____

Address (Street, City, State, Zip): _____