



Nonprofit Entity Advantage

Massachusetts New Business Application

Underwritten by The Hanover Insurance Company

NOTICE: THIS APPLICATION IS FOR A CLAIMS-MADE POLICY. SUBJECT TO ITS TERMS, THIS POLICY WILL APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD. PLEASE READ THE POLICY CAREFULLY.

I. APPLICATION 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.
- Include all requested underwriting information indicated in Section XIII. below.
- Complete the relevant sections of this application and any Supplemental Applications in accordance with the coverages being requested.

II. GENERAL INFORMATION

- Name of Applicant: _____
- Address of Applicant: _____
 City: _____ State: _____ Zip Code: _____ Telephone: _____
- 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: _____
- Individual responsible for human resources or employment law matters (*Loss Prevention services contact*):
 Name: _____ Title: _____
 E-Mail Address: _____ Telephone: _____
- State of incorporation: _____ Date established: _____
- Describe the Applicant's operations:

- Does the applicant have any of the following:

a. Subsidiaries domiciled outside the U.S.?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Branch or representative offices outside the U.S.?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Joint ventures or partnerships with third parties outside the U.S.?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Revenue or donations originating outside the U.S.?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

If "Yes", please attach details including the country(ies), nature of operations, and names of venture partners including percentage ownership.
- Within the past 3 years, has there been any change (resignations, departures, retirements, etc.) in the position of the Chairman of the Board, Executive Director, President, Chief Executive Officer or Chief Financial Officer (or equivalent positions)? Yes No
If "Yes", please attach the following details: Name of individual(s); date of change; and reason for change.
- In the next 12 months (or during the past 18 months) is the Applicant contemplating (or has the Applicant completed or been in the process of completing):



- a. Any merger, acquisition, or divestment? Yes No
 - b. Any change in outside auditors? Yes No
 - c. Any reorganization or arrangement with creditors under federal or state law? Yes No
 - d. Any branch, location, facility, office, or subsidiary closings, consolidations or layoffs? Yes No
- If "Yes" to any part of Question 9, please attach an explanation.*

10. Does the Applicant have any subsidiaries for which coverage is requested? Yes No
If "Yes", please attach a list of these entities and indicate nature of business for each.

IMPORTANT: It is understood and agreed that coverage is not provided for subsidiaries in Question 10 unless the information requested above is provided.

11. Does the Applicant currently have tax-exempt status under the U.S. Internal Revenue Service Code? Yes No
 If "Yes" under which IRSC Section? _____
 If "No" please attach a full explanation.

12. Does the applicant:
- a. Provide any professional services, including but not limited to, legal counseling or medical care? Yes No
 - b. Conduct peer review, standard setting, certification, accrediting, or credentialing activities? Yes No
 - c. Promote, sponsor or provide any form of insurance to its members or non-members? Yes No
 - d. Transact electronic commerce on behalf of itself, members or third parties? Yes No
 - e. Have membership in any nonprofit or professional associations? Yes No
 - f. Operate or sponsor a Political Action Committee (PAC)? Yes No
- If "Yes" please attach a full description of details.*

13. Is the Applicant in compliance with all debt and/or loan covenants? Yes No
If "No" please attach a full explanation

14. Please complete the following financial information for the most recent fiscal year (indicate month/year):
 ____ Month ____ Year, or check box if attaching most recent year-end financial statements instead:

Financial Data	Current Year	Previous Year
Total Assets:	\$	\$
Fund Balance (Net Assets):	\$	\$
Total Revenue:	\$	\$

15. Please provide the following information regarding the Applicant's employees.

Number of Employees	Current Year	Previous Year
Full Time (include Independent Contractors):		
Part Time (include leased and seasonal):		
Volunteers:		
Located in California:		
Located outside the U.S.:		



III. REQUESTED COVERAGE

Indicate below which coverages are being requested. **Complete only those sections of this Application which pertain to requested coverage.**

Coverage Part		Requested Limit(s)
<input type="checkbox"/>	Directors & Officers and Entity Liability	\$
<input type="checkbox"/>	Employment Practices Liability	\$
<input type="checkbox"/>	Fiduciary Liability	\$
<input type="checkbox"/>	Crime Coverage	\$
<input type="checkbox"/>	Cyber Privacy & Security Coverage	\$
<input type="checkbox"/>	Kidnap & Ransom Coverage	\$

IV. CURRENT INSURANCE INFORMATION

Please provide the following information regarding the Applicant's most recent insurance. If no coverage is currently in place, please indicate with "N/A".

IMPORTANT: The **Insurer** will rely upon the declarations and statements contained in any prior application(s) submitted and the Applicant understands and agrees that those declarations and statements will be incorporated into any policy issued by the **Insurer**.

Coverage Part	Insurer	Coverage Date*	Limit(s) of Liability	Retention	Premium	Expiration Date
Directors & Officers Liability			\$	\$	\$	
Employment Practices Liability			\$	\$	\$	
Fiduciary Liability			\$	\$	\$	
Crime Coverage		N.A.	\$	\$	\$	
Cyber Privacy & Security Coverage			\$	\$	\$	
Kidnap & Ransom			\$	\$	\$	

* Coverage Date refers to the "Prior & Pending Date, "Prior Acts Date", "Retroactive Date" or similar term shown on the declarations page of the current policy.

- 1. Has the Applicant exercised any Extended Reporting Period (or Discovery Period) for any Coverage Parts to which this application relates? Yes No
- 2. Within the past 5 years has the Applicant given notice of any claim, circumstance, or potential claim to any insurer under any of the coverage parts to which this application relates? Yes No
If "Yes", please attach a full explanation of the claim, circumstance, or potential claim.
- 3. Within the past 5 years has the Applicant cancelled or non-renewed any coverage parts to which this application relates? **(Not Applicable In Missouri)** Yes No
If "Yes", please explain.

V. DIRECTORS AND OFFICERS LIABILITY INFORMATION

- 1. During the past 5 years, has the Applicant or any organization or person proposed for coverage been the subject of, or been involved in, any of the following:
 - a. Anti-trust, copyright or patent litigation? Yes No
 - b. Civil, criminal or administrative proceeding alleging violation of any Federal or State laws? Yes No
 - c. Civil, criminal or administrative proceeding alleging violation of any Federal or State Anti-Trust or Fair Trade Law? Yes No
 - d. Any other criminal actions? Yes No
 - e. Any action for suspension or revocation of a license, authority or for any professional disciplinary sanction? Yes No*If "Yes" to any of the above in Question 1, attach a full description of the details.*
- 2. Other than those identified in your response to Question 1 above, has any claim been brought at any time during the last 5 years against (i) any Applicant or (ii) any proposed insured individual in his or her capacity as a director or officer of any entity? Yes No
If "Yes" please attach a full description of the details.
- 3. Does the Applicant hold any patents? Yes No
If "Yes" please attach a list and description.

VI. EMPLOYMENT PRACTICES LIABILITY INFORMATION

- 1. What percentage of the Applicant's Employees currently earn more than \$100,000? ■ %
- 2. Does the Applicant have written procedures in place regarding:
 - a. Equal Opportunity Employment: Yes No
 - b. Anti- Discrimination Yes No
 - c. Anti-Sexual Harassment Yes No
 - d. Employment at Will: Yes No
 - e. Progressive Discipline: Yes No
 - f. Handling complaints of sexual harassment or discrimination: Yes No
 - g. ADA accommodations: Yes No
- 3. Does the Applicant:
 - a. Distribute and document the receipt of an employee handbook to all employees? Yes No
 - b. Have written procedures in place that are distributed to each employee if the Applicant does not have an employee handbook? Yes No
 - c. Conduct performance evaluations to determine if an employee will maintain his/her employment or be considered for a promotion? Yes No
If "Yes", please attach a full description with details.
 - d. Have a full-time human resources manager or department? Yes No

- e. Review all terminations with human resources or in-house / outside counsel? Yes No
- f. Conduct training regarding anti-discrimination and anti-sexual harassment policies and procedures using in-house human resource staff or an outside vendor? Yes No
- 4. During the past 5 years, has any Applicant in any capacity, been involved in any lawsuit, charges, inquiries, investigations, grievances or other administrative hearings or proceedings before any of the following agencies and/or any of the following forums, including both domestic and foreign equivalents? Yes No
 - a. National Labor Relations Board? Yes No
 - b. Equal Employment Opportunity Board? Yes No
 - c. Office of Federal Contract Compliance Programs? Yes No
 - d. U.S. Department of Labor? Yes No
 - e. Any State or Local Government agency such as the Labor Department or Fair Employment Agency? Yes No
 - f. U.S. District or State Court? Yes No

If "Yes" to any of the above in Question 4, please attach a full description with details.
- 5. Does the Applicant have established policies and procedures:
 - a. Outlining employee conduct when dealing with third parties, including non-discrimination and non-harassment statements? Yes No
 - b. Outlining independent contractor conduct when dealing with third parties, including non-discrimination and non-harassment statements? Yes No
 - c. For responding to complaints of harassment, discrimination or civil rights violations from third parties? Yes No
- 4. What percentage of the Applicant's employees work at customer locations or perform a majority of their functions off-site? _____ %
- 5. During the past 5 years, has the Applicant had any action or civil suit brought against them by a customer, client or third party alleging harassment, discrimination, or civil rights violations? Yes No
If "Yes" please attach a full description of the details.
- 6. What is the percentage of employee turnover in the last twelve months? _____ %

VII. FIDUCIARY LIABILITY INFORMATION

1. Please list the names and types of **Applicant's** employee benefits plan(s). Attach additional pages if needed.

Plan Names (Do not include health & welfare plans)	Plan Assets (Most current year)	Type of Plan*	Funding (DB only) Under or Over Funded by more than 25%	Number of Plan Participants	Third Party or Outside Administrators
			<input type="checkbox"/> Yes <input type="checkbox"/> No		
			<input type="checkbox"/> Yes <input type="checkbox"/> No		
			<input type="checkbox"/> Yes <input type="checkbox"/> No		

* *Defined Contribution (DC), Defined Benefit (DB), Employee Stock Ownership (ESOP), Excess Benefit or Top Hat (EBP)*

- 2. Does the Applicant handle any investment decisions in-house?
If "Yes," please describe: _____ Yes No
- 3. If "No" to question 2 above, do the fiduciaries review the investment guidelines used by the investment managers at least annually? Yes No
- 4. Are all plans in compliance with plan agreements and ERISA?
If "No," please describe: _____ Yes No



5. Has any employee benefit plan:
- a. Invested in securities of the Applicant? Yes No
 - b. Invested in more than 10% of any entity other than the Applicant or a pooled investment vehicle such as a mutual fund? Yes No
 - c. Loaned or pledged any employees benefit plan assets to any party-in-interest (including the Applicant)? Yes No
- If "Yes" to any of the above in Question 5, please attach a full description with details.*
6. Are there any overdue Applicant contributions for any plan, or has any plan requested or contemplated filing a request for a waiver of contributions? Yes No
If "Yes", please attach a full description with details.
7. Within the last 3 years, has there been, or is there currently under consideration, any restructuring, spin-off, transfer, consolidation, merger, termination or other similar transaction of any employee benefit plan? Yes No
If "Yes", please attach a full description with details.
8. Are all employee welfare benefit plans compliant with the Health Insurance Portability and Accountability Act (HIPAA)? Yes No
9. Does the plan sponsor comply with the summary plan description requirements under ERISA for all employee benefit plans? Yes No
10. Do all employee benefit plans have a written investment policy? Yes No
11. Is the "fair market value" of all employee benefit plans calculated annually? Yes No
If "No" to any of the above in Questions 8-11, please attach a full description with details.
12. During the past 5 years, has there been, or is there currently, any investigation by the IRS, Department of Labor (DOL) Pension Benefit Guarantee Corporation (PBGC), or any other State or Federal Agency of any employee benefit plan or any current or former fiduciary of such employee benefit plan? Yes No
If "Yes" please attach a full description of the details.

VIII. CYBER PRIVACY AND SECURITY COVERAGE

1. Please provide the following:

Number of Donor/Customer/Patient Records: _____
 Number of Online Customers: _____
 Total Number of IP Addresses Assigned: _____
 Number of Active IP Addresses: _____
 Gross Revenue from on-line donations, sales or services: _____
 Estimated Number of Credit Card Transactions if applicable: _____

2. Requested Coverage

Insuring Agreement	Requested Limit	Requested Retention
Privacy and Security Liability	\$	\$
Cyber Media Liability	\$	\$
Breach Event Expenses	\$	\$
Breach Reward Expenses	\$	\$

Breach Restoration Expenses	\$	\$
Cyber Investigations	\$	\$
Cyber Business Interruption	\$	\$
Cyber Extortion	\$	\$
Cyber Theft	\$	\$

3. Please indicate the type of information that the Applicant collects and which resides on the Applicant's or service provider's systems and networks.
- | | | |
|---|--|---|
| <input type="checkbox"/> Credit Card Numbers | <input type="checkbox"/> Race, Ethnicity, National Origin | <input type="checkbox"/> Salary and Compensation |
| <input type="checkbox"/> Social Security Numbers | <input type="checkbox"/> Data Regarding Sexual Orientation | <input type="checkbox"/> Criminal Records |
| <input type="checkbox"/> Email Addresses | <input type="checkbox"/> Account Numbers | <input type="checkbox"/> Disability Status |
| <input type="checkbox"/> Medical Information | <input type="checkbox"/> Financial Data (i.e. credit rating) | <input type="checkbox"/> Civil Judgments |
| <input type="checkbox"/> National ID Numbers | <input type="checkbox"/> Passwords, Including PINs | <input type="checkbox"/> Clients' Intellectual Property |
| <input type="checkbox"/> Drivers' License Numbers | <input type="checkbox"/> Usernames | |
4. Does the applicant utilize third-party service providers for:
- | | |
|---|--|
| a. Back up of electronic data? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| b. Web-site hosting? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| c. Processing or maintenance of sensitive data: | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| d. Maintenance of applications? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| e. Infrastructure hosting? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
- If "Yes" to any of the above please attach a list of providers and services offered.*
5. With respect to the written contracts with the service providers identified in Question 33:
- | | |
|--|--|
| a. Are contracts reviewed by in-house or outside counsel? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| b. Do contracts require the Applicant to be indemnified and "held harmless" for the errors or omissions of the service provider? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| c. Is the service provider required to carry errors & omissions insurance or "cyber liability" insurance? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| d. Is the liability of the service provider limited or restricted in any manner? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
6. Has the applicant evaluated the level of security provided by any of the service providers used per the question above?
- | | |
|--|--|
| a. Review of SAS Type I or SAS Type II | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| b. Review of SSAE 16 | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| c. Review of security audit conducted by third party | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| d. Other, please describe: | <input type="checkbox"/> Yes <input type="checkbox"/> No |
-
7. Does the Applicant have an information security policy? Yes No
8. Does the Applicant's information security policy identify and proscribe the type and level of protection for all of the Applicant's information assets, electronic and physical, whether held by the Applicant or by a person or organization providing services to the Applicant? Yes No
9. Does the Applicant's information security policy include the following?
- | | |
|---|--|
| a. Defined duties and responsibilities of an Information Security Officer | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| b. Requirements for confidentiality agreements for employees, vendors and contractors | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| c. Document classification protection and destruction protocols | <input type="checkbox"/> Yes <input type="checkbox"/> 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

- 10. Are all users of the Applicant's network issued unique passwords?
 If "Yes" are passwords subject to enforced password complexity and change requirements? Yes No
Yes No
- 11. 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
- 12. Does the Applicant have policies regarding the following?
 - a. Internet usage Yes No
 - b. Use of social networking sites or applications Yes No
 - c. E-mail usage Yes No
 - d. Privacy Yes No
 - e. Are employees required to acknowledge that they are aware of such policies listed in a-d above? Yes No

- 13. Are penetration tests and vulnerability scan tests conducted on the Applicant's public-facing network at least annually? Yes No
- 14. Does the Applicant's management review the following for prospective personnel who will have access to sensitive information?
 - a. Criminal history records Yes No
 - b. Credit history records Yes No
 - c. Previous employment records Yes No
- 15. Do individuals other than employees have access to sensitive information? Yes No
- 16. Are all rooms that contain main frames, servers, switches or routers locked with access permitted with a key card or some other device that can be logged? Yes No
- 17. Does the Applicant investigate patterns of attempted access by persons who should not have access to equipment described above? Yes No
- 18. Is the identity of all visitors verified prior to granting them access to the Applicant's premises where sensitive information or the network can be attained? Yes No
- 19. Is sensitive customer (or patient) data stored on web servers? Yes No
- 20. Does the Applicant employ web application firewalls. Yes No
- 21. Does the Applicant utilize a contemporary intrusion detection/prevention system (IDS/IPS) solution as part of the primary firewall or as a separate free-standing solution? Yes No
- 22. Are web servers housed in a dedicated DMZ? Yes No
- 23. Is external access to sensitive information encrypted using SSL? Yes No
- 24. When are the Applicant's applications assessed for vulnerabilities such as SQL injections, cross-site scripting and buffer overflow?
 - a. During development Yes No
 - b. Before deployment Yes No
 - c. Regularly after deployment Yes No
- 25. How quickly does the Applicant remediate vulnerabilities after they are discovered? _____
- 26. Are session lifetimes limited? Yes No

27. Can the Applicant be alerted or otherwise identify when personally identifiable private or health information or confidential information is downloaded to a mobile memory device or sent in an email or added as an attachment to email? Yes No
28. Are company or employee-owned smartphones governed by the Applicant using a contemporary mobile device management (MDM) solution? Yes No
29. Regarding the Payment Card Industry Data Security Standard (PCI DSS):
- a. Has a PCI certified Security Assessor performed an assessment of the Applicant's security within the past year? Yes No
 - b. If "No" to 29.a. above has the Applicant completed a fully compliant Self-Assessment Questionnaire (SAQ)? Yes No
 - c. Have all critical recommendations been corrected or complied with? Yes No
 - d. If "no" when will all critical recommendations be corrected or complied with?
-
30. If the Applicant is a healthcare organization:
- a. Is the Applicant a covered entity under the Health Insurance Portability and Accountability Act (HIPAA)? Yes No
 - b. Is the Applicant a Business Associate under the HIPAA? Yes No
 - c. If "Yes" to the questions above, approximately how many individuals' Protected Health Information do you collect, store or process?
-
- d. If "Yes" to the questions above is the applicant in full or partial compliance with the provisions of the HITECH Act? Yes No
 - e. If the Applicant is in partial compliance with the HITECH Act when will the Applicant be in full compliance?
-
31. 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 HIPAA Privacy Rule or Security Rule? Yes No
- a. If "Yes" was the Applicant found to be in compliance? Yes No
 - b. If "No" please indicate which areas the Applicant was found not to be in compliance.
-
32. Is sensitive information collected through hand written applications, forms or notes? Yes No
- a. If "Yes" are documents shredded after entering the information into a computer system? Yes No
 - If "No" does the Applicant:
 - b. Retain the documents in secured files? Yes No
 - c. Store documents in secure areas that minimize access by persons not authorized to view such documents? Yes No
 - d. Enforce a "clean desk" policy? Yes No
 - e. Shred documents when they are ultimately disposed of? Yes No
33. Is sensitive information in any written form stored with a third party? Yes No
- a. If "Yes" does the applicant have a written contract with the respective service providers? Yes No
 - b. If "Yes" does the Applicant's contract with the service provider state that the service provider:
 - 1) Has Primary responsibility for the security of the Applicant's information? Yes No
 - 2) Has a contractual responsibility for any losses or expenses associated with any failure to safeguard the Applicant's information? Yes No

34. Does the Applicant have an Incident Response Plan (IRP)? Yes No
 If "Yes" does the IRP address:
- a. Unauthorized access to the Applicant's computers, system network or any 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 and system outages? Yes No
 - d. Extortion demands? Yes No
 - e. Corruption of or damage to, electronic data? Yes No
35. Has the IRP been reviewed and approved by the Applicant's board of directors? Yes No
36. Does the plan include a review of the applicable state or federal laws or regulations with which the Applicant may have to comply? Yes No
37. Is the IRP tested annually? Yes No
38. Is there a specific person or group of persons responsible for maintaining the IRP? Yes No
39. Does the IRP identify:
- a. The organizations that will provide mailing or other notification services? Yes No
 - b. The organizations that will provide public relations services? Yes No
 - c. The organizations that will provide credit or other monitoring services? Yes No
 - d. The organizations that will provide forensic services? Yes No
40. Does the Applicant have a Business Continuity Plan? Yes No
 If "Yes":
- a. Is the plan reviewed and updated annually? Yes No
 - b. Is the plan tested at least annually? Yes No
 - c. Have recovery time/point objectives (RTO/RPO) been established for high-priority and/or mission-critical systems or applications? Yes No

IX. CRIME COVERAGE

1. Requested Coverages

Insuring Agreement	Requested Limit	Requested Retention
Fidelity		
Employee Theft	\$	\$
ERISA Fidelity	\$	\$
Client Property	\$	\$
Forgery Or Alteration	\$	\$
Premises Coverage	\$	\$
Transit Coverage	\$	\$
Computer Crime		
Computer Fraud	\$	\$
Program and Electronic Data Restoration	\$	\$

Funds Transfer Fraud	\$	\$
Credit, Debit or Charge Card Fraud	\$	\$
Money Orders and Counterfeit Money	\$	\$
Personal Accounts Protection		
Forgery or Alteration	\$	\$
Identity Fraud Expense Reimbursement	\$	\$
Investigative Expense	\$	\$

2. Does the Applicant:
- a. Allow the employees who reconcile the monthly bank statements to also:
 - 1) Sign checks? Yes No
 - 2) Handle deposits? Yes No
 - 3) Have access to check signing machines or signature plates? Yes No
 - b. Require countersignature of checks? Yes No
 If "Yes", over what amount? \$ _____
 If "No", who can sign checks? _____
 - c. Design internal controls so that no employee can control a process from beginning to end (e.g. request a check, approve a voucher or sign a check)? Yes No
 - d. Store check stocks under dual control with controlled access? Yes No
 - e. Immediately stamp incoming checks "For Deposit Only"? Yes No
3. Does an annual external audit include all subsidiaries and joint ventures? Yes No
4. Does the Applicant's external audit include all of its locations? Yes No
 If "No," please describe: _____
5. Does an independent CPA provide a Management Letter to the Applicant? Yes No
6. Is there a documented system of internal control policies/procedures? Yes No
7. Is there an internal audit department? Yes No
8. Are management policies and computer system controls in place to prevent individual(s) who approve new hires from adding them into the payroll? Yes No
9. Do you have a program in place to detect possible "Ghost" employees? Yes No
10. How often does the Applicant perform a physical inventory check of stock and equipment?

 Who performs these reconciliations? _____
11. Does the Applicant maintain a perpetual inventory of stock, including raw materials/manufactured or purchased goods/scrap? Yes No
12. Are internal control policies and procedures for foreign locations consistent with those of domestic locations? Yes No
 If "No", please attach an explanation.
13. Does the Applicant perform pre-employment reference checks for all its potential employees? Yes No
 If "No", please attach an explanation
14. Does the Applicant:
- a. Maintain a list of authorized vendors? Yes No



- b. Have a procedure in place to verify the existence and ownership of new vendors? Yes No
- c. Allow the same individual who verifies the existence of vendors to also have the authority to edit the authorized master vendor list? Yes No
- d. Verify invoices against a corresponding purchase order, receiving report and the authorized master vendor list prior to issuing payment? Yes No

- 15. Are the duties of computer programmers and operators separated? Yes No
- 16. Has separation been established between authority to initiate and approve a wire transfer? Yes No
- 17. If a telephone call can activate a transfer of funds, does your financial institution call an employee other than the one who requested the transfer before acting on the transfer request? *If "Yes", what is the callback threshold?* _____ Yes No
- 18. Are transfer verifications sent to an employee or a department other than the one who initiated the transfer? Yes No
- 19. Are wire transfers reconciled the same day the transfer verifications are received by an individual who did not approve or transmit such wire transfer? Yes No
- 20. Are the following physical controls in place?
 - a. Alarm System Yes No
 - b. Video Cameras Yes No
 - c. Security Guards Yes No
 - d. Controlled Premises Access Yes No
- 21. Maximum exposure inside the premises:
 Location: _____ Cash: \$ _____ Checks/Securities: \$ _____
- 22. Do you use an Armored Motor Vehicle Company to transport Money or Securities? Yes No
If "No", please complete below:
 Maximum exposure outside the premises:
 Location: _____ Cash/Securities: \$ _____
 Checks: \$ _____ # of Messengers: _____
- 23. List all employee theft, forgery, computer fraud or other crime losses discovered by the Applicant in the last 5 years, itemizing each loss separately. Include date of loss, description, total amount of loss, and corrective measures. *Attach additional pages if needed.* Check if none

- 24. Please describe the services the Applicant provides for clients:

- 25. Do any of the Applicant's clients require the Applicant to carry crime insurance or to be bonded? Yes No
If "Yes", please explain and specify amount.

X. KIDNAP & RANSOM COVERAGE

1. Complete the following information regarding the foreign travel of the Applicant:

Please attach additional pages if needed.

Country Visited	Number of annual trips	Average length of stay	Number of employees traveling	Number of independent contractors traveling

2. Describe the Applicant's security precautions while traveling, both domestic and international, including use of security consultants:

3. Please attach a list of all kidnapping, extortion threats, cyber extortion, hijacking, wrongful detention, or political threats discovered by the Applicant in the last five years, itemizing each loss separately:

Check box if None or describe below and attach additional pages as needed:

XI. PRIOR KNOWLEDGE AND APPLICANT REPRESENTATION

The Applicant must answer the prior knowledge question below:

- For any **Liability Coverage Part** for which coverage is requested and is not currently purchased; or
- If the Applicant is requesting larger limits than are currently purchased.

Is any **Insured** 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 **Liability Coverage Parts**?

Yes No

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

This representation applies only to those coverage types for which no coverage is currently maintained and any larger limits of liability requested.

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

XII. 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.

XIII. DECLARATIONS, NOTICE AND SIGNATURES

The submission of this New Business Application does not obligate the **Insurer** 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 **Insurer** to make any inquiry in connection with this **Application**.

The undersigned, acting on behalf of all Applicants, declare that to the best of their knowledge and belief, after reasonable inquiry, the statements set forth in this **Application** and in any attachments or other documents submitted with the **Application** are true and complete and were made to obtain requested information from each and every Applicant proposed for this insurance to facilitate the proper and accurate completion of this **Application**.

The undersigned agree that the information provided in this **Application** and any material submitted herewith are the representations of all the Applicants and the basis for issuance of the insurance policy should a policy providing the requested coverage be issued, and that the **Insurer** will have relied on all such materials in issuing any such policy. The undersigned further agree that the **Application** and any material submitted herewith shall be considered attached to and a part of the policy. Any material submitted with the **Application** shall be maintained on file (either electronically or paper) with us.

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

NOTICE TO ALABAMA APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution fines or confinement in prison, or any combination thereof.

NOTICE TO ARIZONA AND MISSOURI APPLICANTS: Claim Expenses are Inside the Policy Limits. All claim expenses shall first be subtracted from the limit of liability, with the remainder, if any, being the amount available to pay for damages.

NOTICE TO ARKANSAS, LOUISIANA AND WEST VIRGINIA 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 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 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 HAWAII APPLICANTS: For your protection, Hawaii law requires you to be informed that presenting a fraudulent claim for payment of a loss or benefit is a crime punishable by fines or imprisonment, or both.

NOTICE TO IDAHO AND OKLAHOMA APPLICANTS: 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 KANSAS APPLICANTS: Any person who commits a fraudulent insurance act is guilty of a crime and may be subject to restitution, fines and confinement in prison. 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 or insurance agent or broker, any written statement as part of, or in support of, an application for insurance, or the rating of an insurance policy, or a claim for payment or other benefit under an insurance policy, which such person knows to contain materially false information concerning any material fact thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

NOTICE TO KENTUCKY 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.

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 include imprisonment, fines and denial of insurance benefits.

NOTICE TO MARYLAND APPLICANTS: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or 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 MICHIGAN APPLICANTS: Any person who knowingly and with intent to defraud an insurance company or another 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 act, which is a crime and subjects the person to criminal and civil penalties.

NOTICE TO NEW JERSEY APPLICANTS: Any person who knowingly includes any false or misleading information on an application for an insurance policy or files a statement of claim containing any false or misleading information is subject to criminal and civil penalties.

NOTICE TO NEW MEXICO 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 civil fines and criminal penalties.

NOTICE TO OHIO APPLICANTS: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

NOTICE TO OREGON APPLICANTS: Any person who knowingly and with intent to defraud or solicit another to defraud any insurance company: (1) by submitting an application, or (2) by filing a claim containing a false statement as to any material fact, may be violating state 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 VERMONT APPLICANTS: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

Note: This **Application** must be signed by the chief executive officer or chief financial officer of the Applicant acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Date

Signature

Title



Supporting Documentation: please attach a copy of the following for every Applicant seeking coverage:

- Most recent CPA prepared financial statements
- Most recent CPA Letter to Management and Management's response. If this Letter is not issued, check here:
- Employment Practices Liability (for Applicants with 500 or more employees):
 - Employee handbook
 - Employment application form
 - Most recent EEO-1
 - Third party policies and statements, if requesting such coverage

Produced By: Agent: _____ Agency: _____

Agency Taxpayer ID or SS No.: _____

Agent License No.: _____ Agent Signature: _____

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