

INTEGRATED TECHNOLOGY E&O AND CYBER RISK APPLICATION - MARYLAND

SUBMISSION REQUIREMENTS

- Copies of the Applicant's current contracts or license agreements
- Current audited financial statement
- Five (5) years of currently valued insurance company loss runs

GENERAL INFORMATION (to be completed by all Applicants)

- Applicant Name(as it should appear on policy):
- Street Address:
 City: _____ State: _____ Zip: _____
- Website Address:
- Business Type: Corporation Partnership Joint Venture LLC
- Ownership Structure: Public Private Not-for-Profit
- Year Established: Number of Employees:
- Risk Management Contact: _____ Phone: _____
 Email: _____

SECTION I - COVERAGES (to be completed by all Applicants)

- Select each coverage and indicate the Limit of Liability and Deductible for which the Applicant is applying.

	Coverage	Limit of Liability	Deductible
	Technology Errors & Omissions	\$	\$
	Network Security and Privacy Liability	\$	\$
	Employee Privacy Liability	\$	\$
	Media Liability	\$	\$
	Privacy Regulation Defense and Fines	\$	\$
	Loss of Digital Assets	\$	\$
	Non-Physical Business Interruption	\$	Hours:
	Cyber Extortion Threat	\$	\$
	Security Event Costs	\$	\$
	Cyber Terrorism Coverage	\$	Hours:

- What is the proposed effective date (mm/dd/yyyy) of coverage:
- Does the Applicant currently have a policy in force providing any of the above coverages? Yes No

Coverage	Technology E&O	Media Liability	Network Security/ Privacy Liability	First Party Cyber Expenses
Carrier				
Policy Period				
Limit of Liability	\$	\$	\$	\$
Retention	\$	\$	\$	\$
Retroactive Date				N/A
Premium	\$	\$	\$	\$

SECTION II - REVENUE (to be completed by all Applicants)

- Indicate on what date the Applicant's fiscal year ends:
- Indicate the Applicant's gross annual revenue for the following twelve (12) month fiscal time periods.

Revenue Split	Prior Fiscal Period	Current Fiscal Period	Next Fiscal Period
Domestic	\$	\$	\$
Foreign	\$	\$	\$
Total	\$	\$	\$

SECTION III - SERVICE/PRODUCTS ALLOCATION/DESCRIPTION OF OPERATIONS
(to be completed by all Applicants)

1. Description of operations:

Estimate the total percentage of revenue for the following services and work.

Technology – Software & Services	%	Computers, Electronics, & Hardware	%
All Software Noted Below:		Aircraft/Spacecraft Electronic Components	%
Installed on Customer Systems	%	Circuit Board or Semiconductor Manufacturing	%
Hosted Remotely (SAAS)	%	Computer System Manufacturing	%
Application Service Provider	%	Computer Peripheral/Device Manufacturing	%
Artificial Intelligence Software/Services	%	Computer Maintenance and Repair	%
Billing/ Payment Processing/ E-Commerce	%	Electric Vehicle Charger Sale or Installation	%
Biometric Software or Services	%	Electronic Component Manufacturing	%
Blockchain Based Technology	%	Electronic Device Manufacturing	%
Cloud Data Hosting or Data Backup	%	Industrial Controls/SCADA Systems	%
Co-location without Managed Services	%	Instrument Manufacturing	%
Custom Software Development	%	Office Electronics Leasing/Sale/Service (Copiers, Printers, Managed Print Services)	%
Data Processing & Outsourced Services	%	Optical Instruments/Lens Manufacturing	%
Data Aggregator/Broker/Customer Targeting	%	Recycling/Destruction of Hardware	%
Domain Name Registration	%	Telecommunications Equipment Manufacturing	%
Emergency/911 Call Routing Software	%	Value-Added Resale of Computer or Telecom Hardware	%
IT Managed Service Provider (<i>manage customer IT Networks/ Systems</i>)	%	Other (<i>describe</i>):	%
IT Managed Security Service Provider (<i>manage customer IT security</i>)	%	Distribution & Value Added Resale	%
IT Consulting	%	Computer Equipment & Software Distribution	%
IT Staff Augmentation	%	Electronic Component Distribution	%
Mobile Phone Application Development	%	Value-Added Resale of Computer or Telecom Hardware	%
Network Security Software and Services	%	Value-Added Resale of Software	%
Pre-Packaged Software Development/ Sales	%	Other (<i>describe</i>):	%
System Design and Integration	%	Telecommunication Services	%
Social Media Products/ Services/ Platform	%	All Installation Work Noted Below:	
Technical Support/Repair & Maintenance	%	Performed by the Applicant	%
Training & Education	%	Subcontracted to Others:	%
Web Portal	%	Audio Visual Installation or Integration	%
Website Hosting	%	Alarm Integration (Burglar/Fire)	%
Website Construction and Design	%	Alarm Monitoring Services	%
Other (<i>describe</i>):	%	Data Transport/Bandwidth/Wholesale Access	%
Other (<i>describe</i>):	%	Internet Service Provider	%
Other Professional Services	%	Local & Long Distance Service Provider	%
Accounting or Actuarial Services	%	Telecommunications Consulting	%
Advertising/Content Creation Services	%	Telecommunication System Installation	%
Architect or Engineering Services	%	Video Conferencing Services	%
Business Process Outsourcing (<i>describe services</i>):	%	VOIP Phone System Integration	%
Esports Related Services or Teams	%	Wireless/Cellular Services	%
Legal Services	%	Telecom Tower Service and Installation	%
Warehousing, Logistics, Fulfillment	%	Other (<i>describe</i>):	%
Other (<i>describe</i>):	%	Other (<i>describe</i>):	%
		Other (<i>describe</i>):	%

SECTION VI - QUALITY CONTROL PROCEDURES (to be completed by all Applicants)

1. Who is responsible for handling insurance related matters:

2. Does the Applicant have policies and procedures in place to respond to customer complaints? Yes No
3. Does the Applicant utilize an escalation procedure to respond to customer complaints? Yes No
4. Indicate which of the quality control procedures are in place. (select all that apply)

Alpha Testing	Customer Service via E-Mail
Beta Testing	Formalized Training for New Hires
Business Continuity Plan	Prototype Development
Customer Screening Process	Vendor Certification Process
Customer Service via a Toll-Free Number	Written Quality Control Guidelines
Customer Service via a Web Portal	Other:
5. Does the Applicant have a disaster recovery/business continuity plan? Yes No
How often do they test it:
6. How often does the Applicant backup critical data and systems?

No backups	Quarterly full backups	Daily/Weekly full/incremental backups
------------	------------------------	---------------------------------------
7. Are backup files stored in a secure location? Yes No
Where: Onsite Offsite Secondary backup hotsite

SECTION VII - SUBCONTRACTED WORK, USE OF SUPPLIERS AND OUTSOURCED MANUFACTURING (to be completed by all Applicants)

1. Does the Applicant sub-contract any professional services or manufacturing to fulfill commitments to clients? Yes No
2. If yes, what percentage does the Applicant subcontract: %
3. Does the Applicant utilize a standard sub-contractor agreement? Yes No
4. Does the Applicant require evidence of General Liability from subcontractors? Yes No
5. Does the Applicant require evidence of Errors & Omissions insurance from subcontractors? Yes No

SECTION VIII - MEDIA (Complete only if applying for Media Liability)

N/A

Business Activities or Website Contents	% of Receipts	Business Activities or Website Contents	% of Receipts
Advertising/Marketing for Others	%	Music or Sound Clips	%
Social Media Services	%	Sexually Explicit Material	%
File Sharing	%	Sweepstakes or Coupons	%
Interactive Gaming	%	Video Production	%
Movie/Commercial Production	%	Other (<i>describe</i>):	%
Website/ Social Media Content	%	Open Source	%
Content created by Applicant	%	Open Source Code originated by Applicant	%
Content supplied by Client	%	Open Source Code created by others and used by Applicant	%
Domain Name Registration	%		

1. If the Applicant distributes computer systems with software included, are the appropriate license agreements supplied with each system? N/A Yes No
2. Does the Applicant produce original content as part of their business such as advertising ideas, content creation services, logo/brand development? N/A Yes No
 - a. If yes, please describe:

 - b. If yes, does the Applicant utilize Generative AI in producing original content? N/A Yes No

3.	Does the Applicant provide social media content services or provide a social media platform for others to post content? a. If yes, please describe:	N/A	Yes	No
4.	Does the Applicant offer comparisons of their product/service to competing products/services?	N/A	Yes	No
5.	Does the Applicant have a procedure for reviewing all content that is disseminated via their website?		Yes	No
6.	Does the Applicant's website, or any website managed by them, include chat rooms, bulletin boards, or blogs? a. If yes, does the Applicant review and edit prior to posting? b. Does the Applicant have a formal procedure for removing controversial or infringing material?		Yes	No
7.	Has the Applicant received notification that any of their material or services infringe on the intellectual property rights of others?		Yes	No
8.	Risk Management Procedures for all Media Activities a. Does the Applicant employ an in-house counsel who specializes in intellectual property rights? b. Does the Applicant have written intellectual property clearance procedures? c. Does the Applicant acquire all necessary rights, licenses or consent to use of content? d. Does the Applicant require employees and contractors to sign a statement that they will not use previous employers' or clients' intellectual property? e. Does the Applicant have agreements in place with contractors, working on their behalf, granting the Applicant ownership of all intellectual property developed for them?		Yes	No

SECTION IX - INFORMATION SECURITY <i>(Complete only if applying for Network Security & Privacy Liability Coverage, or if Applicant is responsible for non-public information on behalf of others.)</i>	N/A
--	------------

Please indicate which type of third party sensitive information resides in the Applicant's network: (Select all that apply)

- Credit card data only for the duration of a transaction then deleted
- Credit card data stored for future use (all but last four (4) digits masked)
- Credit card data stored for future use (un-masked card numbers or including track two (2) data)
- Private health information
- Sensitive or proprietary company information (including trade secrets)
- Bank Account or Financial Records
- Employee/HR Information
- Customer Login Information (usernames with unmasked passwords)
- Other personally identifiable financial information (*describe*):

Total number of individual Third Party Sensitive Information records above:

BASIC SECURITY

1.	Does the Applicant have anti-virus deployed across their network with automatic updates?	Yes	No
2.	Does the Applicant have a firewall in place? If yes, is it configured to disallow inbound connections by default?	Yes	No
3.	Are critical software and network vulnerabilities patched within 30 days?	Yes	No
4.	Does the Applicant encrypt all data at rest, in-transit, and on all portable devices which store personal data?	Yes	No
5.	Is the Applicant currently up to date with any relevant regulatory and industry framework such as: Payment Card Industry (PCI), Portability & Accountability Act (HIPAA), Gramm-Leach Bliley, CAN-SPAM Act, or similar?	Yes	No

ADDITIONAL SECURITY

- | | | |
|---|-----|----|
| 1. Are access controls employed using the principle of least privilege? | Yes | No |
| 2. Is critical data backed up physically disconnected "offline" from the internet? | Yes | No |
| 3. Please confirm that the Applicant has <i>NO</i> open Remote Desktop Ports (RDP's). | Yes | No |
| 4. Does the Applicant require the use of multi-factor authentication (MFA) for: | Yes | No |
| a. All remote access (including employees, vendors, and third parties)? | Yes | No |
| b. Privileged users? | Yes | No |

ADVANCED SECURITY

- | | | |
|--|-----|----|
| 1. Does the Applicant utilize any next generation anti-virus or behavioural analysis including Endpoint Detection and Response (EDR)? | Yes | No |
| a. If yes, please state which product used (such as CrownStrike Falcon, SentinelOne): | | |
| 2. Are employees trained in phishing and social engineering techniques?
How often? | Yes | No |
| 3. Does the Applicant utilize email filtering tools such as: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting and Conformance)? | Yes | No |

ADMINISTRATIVE SECURITY

- | | | |
|--|-----|----|
| 1. Does the Applicant have a formal incident response plan? | Yes | No |
| 2. Does the Applicant have a formal process for approving and testing all external network connections through their firewall? | Yes | No |
| 3. Does the Applicant have a Chief Information Officer or Chief Information Security Officer or equivalent management role responsible for IT Security and/or compliance? | Yes | No |
| 4. Has the Applicant undergone an IT security/privacy evaluation/assessment or audit?
Were any found deficiencies corrected? | Yes | No |
| 5. Does the Applicant allow storage of non-public personal or commercial information on portable devices or media? | Yes | No |
| 6. Does the Applicant limit server and data center access to only authorized personnel? | Yes | No |
| 7. Is remote access for portable devices restricted to Virtual Private Networks (VPNs)? | Yes | No |
| 8. Does the Applicant have an established procedure for employee departure that includes an inventoried recovery of all information assets, user accounts, and systems access assigned to the individual? | Yes | No |
| 9. Does the Applicant have a written private policy? | Yes | No |
| 10. Does the Applicant outsource all payment processing to a PCI-DSS validated merchant or entity? | Yes | No |
| a. What are the Applicant's estimated number of transactions in a 12-month period? | | |
| b. Has the Applicant been PCI certified in the past 12 months? | Yes | No |
| 11. Does the Applicant require employees to authenticate any requested changes to established vendor, supplier, or customer information (such as: bank account, routing number, contact information) via:
Predetermined call-back number: _____ Other control (describe): _____ | Yes | No |
| 12. Is dual authorization required for all wire transfers?
If yes, above what amount? \$ _____ | Yes | No |
| 13. Provide the average daily dollar amount of wire transfers: \$ _____ | | |
| 14. Does the Applicant have any single source providers of raw materials, products, or services (such as: communications, hosting, managed services) which are critical to their business? | Yes | No |
| a. If yes, please describe: | | |
| b. If any of the above providers of raw materials, products, or services failed to deliver as agreed, how quickly would the Applicant be able to secure replacement services? | | |

- | | |
|---|------------------------------|
| 15. Does the Applicant replace factory default settings to ensure information security systems are securely configured? | Always
Sometimes
Never |
| 16. Does the Applicant retain personally identifiable information only for as long as needed? | Always
Sometimes
Never |
| 17. Does the Applicant discard personally identifiable information when no longer needed by irreversibly erasing or destroying the data using a technique that leaves no residual data? | Always
Sometimes
Never |
| 18. Does the Applicant require third parties to whom they entrust personally identifiable information to contractually agree to protect such information using safeguards at least equivalent to their own? | Always
Sometimes
Never |
| 19. Does the Applicant's hiring process include conducting background checks on employees? | Always
Sometimes
Never |

SECTION X - HISTORICAL BUSINESS INFORMATION (to be completed by all Applicants)

- | | | |
|--|-----|----|
| 1. Does the Applicant have any account receivables for professional or technology service contracts that are more than ninety (90) days past due?
If yes, attach details. | Yes | No |
| 2. Within the past five (5) years, has the Applicant sued any customers for non-payment of any contract or licensing fee?
If yes, attach details. | Yes | No |
| 3. Within the past five (5) years, have any customers withheld payment or requested a refund of fees because the Applicant's products/ services: | | |
| a. Did not meet customer's performance expectations? | Yes | No |
| b. Did not perform in compliance with the Applicant's warranty or guarantee? | Yes | No |
- If yes, attach details.**

**SECTION XI - HISTORICAL CLAIMS & INVESTIGATORY INFORMATION
(to be completed by all Applicants)**

- | | | |
|---|-----|----|
| 1. Have any technology errors and omissions, media liability, or network security/ privacy injury claims been made during the past five (5) years against the Applicant?
If yes, attach a detailed summary, including the name of the claimant, the date the claim occurred, the date it was reported, the demand amount, whether the claim is open or closed, and the amount paid by both the insured and insurance. | Yes | No |
| 2. Does the Applicant's Chief Executive Office, Chairperson, Chief Financial Officer, President, or Risk Manager have knowledge, information of any circumstance, or aware of any incident or security breach that could give rise to a claim, breach incident, or extortion that would be covered by this policy?
If yes, attach a detailed summary, including the name of the claimant or breach details, the date the claim or breach occurred, the date it was reported, the demand amount, and any other pertinent details. | Yes | No |
| 3. Has the Applicant received any complaints, claims, or been subject to litigation involving matters of privacy injury, intellectual property infringement, denial of service attacks, computer virus infections, theft or information, damage to third party networks or their customers' ability to rely on their network?
If yes, attach details. | Yes | No |
| 4. Within the last five (5) years, has the Applicant been the subject of an investigation or action by any regulatory or administrative agency arising out of their business practices?
If yes, attach details. | Yes | No |

FRAUD STATEMENT AND SIGNATURE SECTIONS

The Undersigned states that they/them are an authorized representative of the Applicant and declares to the best of their knowledge and belief and after reasonable inquiry, that the statements set forth in this Application (and any attachments submitted with this Application) are true and complete and may be relied upon by Company * in quoting and issuing the policy. If any of the information in this Application changes prior to the effective date of the policy, the Applicant will notify the Company of such changes and the Company may modify or withdraw the quote or binder. In Maryland, a binder or policy is subject to a 45-day underwriting period beginning on the effective date of coverage. We may cancel a binder or policy during the underwriting period if the risk does not meet our underwriting standards of the insurer. If we discover a material risk factor during the underwriting period, we shall recalculate the premium for the policy or binder based on the material risk factor as long as the risk continues to meet the underwriting standards of the insurer.

The signing of this Application does not bind the Company to offer, or the Applicant to purchase the policy.

*Company refers collectively to Philadelphia Indemnity Insurance Company and Tokio Marine Specialty Insurance Company

VIRGINIA APPLICANT: READ YOUR POLICY. THE POLICY OF INSURANCE FOR WHICH THIS APPLICATION IS BEING MADE, IF ISSUED, MAY BE CANCELLED WITHOUT CAUSE AT THE OPTION OF THE INSURER AT ANY TIME IN THE FIRST 60 DAYS DURING WHICH IT IS IN EFFECT AND AT ANY TIME THEREAFTER FOR REASONS STATED IN THE POLICY.

FRAUD NOTICE STATEMENTS

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 THAT PERSON TO CRIMINAL AND CIVIL PENALTIES (IN OREGON, THE AFOREMENTIONED ACTIONS MAY CONSTITUTE A FRAUDULENT INSURANCE ACT WHICH MAY BE A CRIME AND MAY SUBJECT THE PERSON TO PENALTIES). **(NOT APPLICABLE IN AL, AR, CA, CO, DC, FL, KS, KY, LA, ME, MD, NJ, NY, OH, OK, PA, RI, TN, VA, VT, WA AND WV).**

APPLICABLE IN AL, AR, LA, MD, RI AND WV: ANY PERSON WHO KNOWINGLY (OR WILLFULLY IN MD) PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR WHO 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/OR CONFINEMENT IN PRISON (IN ALABAMA, MAY BE SUBJECT TO RESTITUTION FINES OR CONFINEMENT IN PRISON, OR ANY COMBINATION THEREOF).

APPLICABLE IN CALIFORNIA: FOR YOUR PROTECTION CALIFORNIA LAW REQUIRES THE FOLLOWING TO APPEAR ON THIS FORM. ANY PERSON WHO KNOWINGLY PRESENTS FALSE OR FRAUDULENT INFORMATION TO OBTAIN OR AMEND INSURANCE COVERAGE OR TO MAKE A CLAIM FOR PAYMENT OF A LOSS IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN STATE PRISON.

APPLICABLE IN COLORADO: 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.

APPLICABLE IN DISTRICT OF COLUMBIA: 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.

APPLICABLE IN FLORIDA 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.

APPLICABLE IN KANSAS: 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.

APPLICABLE IN KENTUCKY: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSONS 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.

APPLICABLE IN MAINE: 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.

APPLICABLE IN NEW JERSEY: ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.

APPLICABLE IN NEW MEXICO: 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.

APPLICABLE IN OHIO: 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.

APPLICABLE IN OKLAHOMA: 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.

APPLICABLE IN PENNSYLVANIA: 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.

APPLICABLE IN TENNESSEE, VIRGINIA AND WASHINGTON: 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.

APPLICABLE IN VERMONT: 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.

APPLICABLE IN 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 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. THIS APPLIES TO AUTO INSURANCE.

NAME (PLEASE PRINT/TYPE)

TITLE
(MUST BE SIGNED BY THE PRINCIPAL, PARTNER, OR OFFICER)

SIGNATURE

DATE

SECTION TO BE COMPLETED BY THE PRODUCER/BROKER/AGENT

PRODUCER
(If this is a Florida Risk, Producer means Florida Licensed Agent)

AGENCY

PRODUCER LICENSE NUMBER
(If this a Florida Risk, Producer means Florida Licensed Agent)

ADDRESS (STREET, CITY, STATE, ZIP)