



## Fran Kelly Professional Liability, LLC Brokerage Agreement

\_\_\_\_\_ (“Client”) hereby designates Fran Kelly Professional Liability, LLC (Producer) to act as your representative in the marketplace to locate certain insurance for Client’s insurance needs. Acting as your representative, Producer will provide to Client various services during this process as described below generally:

- Discuss with you specifics about your insurance needs;
- Assist you, at your request, with questions regarding the completion of any application for insurance;
- Search available markets for an insurer(s) interested in providing insurance;
- Present to you any proposals and/or sample policies or policy summaries of insurers willing to provide a quote offer;
- Facilitate the acceptance process, binder issuance and policy delivery;
- Assist you throughout the policy term by providing assistance and service on the policy as reasonably expected.

**Cyber crime advisory: E&O policies are not intended to cover this exposure. To fully address this risk, we recommend separate cyber and crime policies.**

Our agency as Producer may charge a fee for the placement and/or servicing of your insurance needs. This fee varies based upon the terms and conditions of the various quote offers/proposals we secure and the ultimate acceptance by Client. Our fee, if any, will be disclosed to you at the time of review of the quote offers/proposals. Other fees may be charged by the insurer, general agency, the state or other party(s) in the process. Any such fees will be disclosed at the time a quote/proposal offer is made and can include such items as:

- Policy fee
- Administrative fee
- Insurer fee
- Surplus lines tax
- Surplus lines stamping fee

Client agrees that such fees may be charged and agrees to pay such fees, in addition to the premium, as a condition to coverage and will timely remit such payment when billed. All premium and fees will be disclosed as part of the quote/offer and shall be in writing. Acceptance by Client of the quote/offer constitutes Client’s awareness and acceptance of such fee(s) charges. This Agreement shall apply to renewal of any policy issued as the result of this Agreement but may be revoked by either Client or Producer to be effective at the next annual anniversary date of the policy.

By Producer

By Client

\_\_\_\_\_

\_\_\_\_\_

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

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

# FUSION

## Cyber Insurance Application

### **NOTICE**

This Fusion Cyber Liability Insurance application will be used for the preliminary submission evaluation. When completed, this application will enable the Underwriter to decide whether or not to authorize the quoting or binding of insurance. Please type or print clearly and answer all questions. Attach a separate sheet if there is insufficient space to answer any question fully. Complete all required supplemental forms/applications. "You" and "Your," as used in this application, means the Applicant.

### **I. GENERAL INFORMATION**

Business Name:

Street Address:

City, State, Zip:

Website(s):

### **BUSINESS INFORMATION**

Year Established:

Description of Operations:

NAICS Code:

Total Number of Employees:

Projected Revenues:

Prior 12 Months Revenues:

### **RISK MANAGEMENT CONTACT**

Name:

Title:

Email Address:

Is your network security outsourced or handled by an in-house team?

# FUSION

## Cyber Insurance Application

<b>II. INDICATION UNDERWRITING QUESTIONS</b>	
1. Do you use a cloud provider to store data or host applications?	
2. Do you require employee training on Network Security, Phishing, and Ransomware?	
3. Is sensitive data encrypted "in transit" and "at rest"?	
4. Is MFA required for all remote network access and email access?	
5. Does your organization utilize EDR solutions across your network?	
6. Do you have regular procedures & cadence for backups?	
7. Does your organization have vulnerability management policies to determine the need for patching?	
8. Do you actively test employees on Phishing and Network Security?	
9. Do you have any operations in Cuba, Iran, Afghanistan, Belarus, Myanmar, North Korea, Russia, Syria, Ukraine, Venezuela, or any other country that is under US sanctions?	
10. Do you require employees to obtain secondary authorization for wire transfers greater than \$25,000?	
11. Can you confirm that you have no open claims or have not had any claims in the last three years that incurred greater than \$25,000 in expenses?	

<b>III. SOCIAL ENGINEERING</b>	
12. Do you have a documented process requiring at least two staff members to review and authorize transactions above \$25,000?	
13. Are all requests to alter supplier and customer bank account details verified with a known contact for authenticity?	
14. Do you outsource transfer verification to a third party or software provider? If 'Yes', who? _____	
Additional Information:	

# FUSION

## Cyber Insurance Application

<b>IV. Backups</b>	
15. Are Backups taken to an offline or online backup medium that is only accessible using multi-factor authentication or, if not protected by multi-factor authentication, immutable?	
16. What frequency do you backup systems?	
a) Continuously	
b) Weekly	
c) Monthly	
d) Daily	
17. Are your backups:	
a) Offline air-gapped	
b) Cloud-based	
c) MFA Protected	
d) Encrypted	
e) Tested (Annually or more)	
f) Recoverable within 3 days	
Additional Information:	

<b>V. MFA</b>	
18. Is Remote access to systems allowed?	
19. MFA is implemented and enforced in the following systems:	
a) Remote email access	
b) Remote Network/Virtual Private Network (VPN) access	
c) administrator/privileged user accounts (all)	

# FUSION

## Cyber Insurance Application

d) Administrator/privileged user accounts (where allowed)	
e) Operational Technology (OT)	
20. Do you use a third-party provider for MFA services? If 'Yes', what provider: _____	
Additional Information:	

<b>VI. Employee Training</b>	
21. Do you require annual employee training in network security, social engineering, and phishing?	
22. Do you proactively use Phishing simulation testing on employees?	
23. Is Social Engineering-specific training required for employees who are responsible for wire transfers?	
Additional Information:	

<b>VII. Payment Cards</b>	
24. Do you accept payment through debit and credit cards?	
25. Do you have a Merchant Service Agreement that requires you to comply with PCI-DSS standards?	
26. Is payment card data stored on your network?	
27. Do you utilize a third-party payment processor or point-of-sale system?	
Additional Information:	

<b>VIII. General Security</b>	
28. Are you in compliance with all applicable Privacy Regulations?	
29. Are you retaining less than 1,000,000 Personally Identifiable Records?	

# FUSION

## Cyber Insurance Application

30. Do you enforce procedures to review/remove content that may infringe or violate any intellectual property or privacy right?	
31. Do you have Anti-Virus Software, including automatic updates, in place across your network infrastructure?	
32. Do you have an Incident Response Plan (IRP), Business Continuity Plan (BCP), or Disaster Recovery Plan (DRP) in place? If 'Yes': a) Has this plan been tested? b) Does it set forth specific action items and responsibilities for relevant parties in the event of a cyber incident or data breach?	
33. Do you use an email security filtering tool?	
34. Are Critical security patches deployed within 30 days of vendor release?	
35. Do you install all firewall updates, anti-virus updates, anti-spyware updates, and patches within 30 days?	
36. Do you have Operational Technology (OT) used within your network infrastructure? If 'Yes': a) Are connections between IT and OT networks segmented? b) Is MFA enforced for remote connections to OT networks?	
37. Do you conduct vulnerability scans on all public-facing IP addresses? If 'Yes', what cadence?	
38. Do you have SIEM or SOC in place?	
39. Are firewalls in place across your network?	
40. Do you have an EDR solution in place? If 'Yes', what provider is used? _____	
41. Are all internet-accessible systems (e.g., web-, email servers) segregated from the organization's trusted network (e.g., within a demilitarized zone (DMZ) or a third-party service provider)?	
42. Do your Agreements with third-party service providers require levels of security commensurate with the organization's information security standard?	
43. Do you use a cloud provider to store data or host applications?	

# FUSION

## Cyber Insurance Application

If 'Yes,' is MFA required on cloud-based systems?	
<p>44. Do you use any end-of-life software within your systems or network infrastructure?</p> <p>If 'Yes':</p> <p style="margin-left: 20px;">a) Are these systems connected to the internet?</p> <p style="margin-left: 20px;">b) Has extended support been purchased from vendors for all devices running the end-of-life software?</p>	
45. Are all generic or default passwords changed or removed (e.g. by deploying Microsoft LAPS)?	
Additional Information:	

<b>IX. LOSS HISTORY</b>	
In the past three (3) years, has the Applicant or any other person or organization proposed for this insurance:	
1. Received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of data, damage to third party networks or the ability of third parties to rely on the Applicant's network	
2. Been the subject of any government action, investigation, or other proceedings regarding any alleged violation of privacy law or regulation	
3. Notified customers, clients, or any third party of any security breach or privacy breach	
4. Received any cyber extortion demand or threat	
5. Sustained any unscheduled network outage or interruption for any reason	
6. Sustained any property damage or business interruption losses resulting from a cyber-attack	
7. Sustained any losses due to wire transfer fraud, telecommunications fraud, or phishing fraud	

# FUSION

## Cyber Insurance Application

8. Know of any security breach, privacy breach, privacy-related event or incident, or allegations of breach of privacy that may give rise to a claim	
9. Claims in the past three (3) years that resulted in expenses incurred greater than \$25,000	
Additional Information:	

**X. SIGNATURE & ACKNOWLEDGEMENT**

The Applicant has read the preceding and understands that completing this application does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this application is complete and correct to the best of the Applicant's knowledge and belief, and that all particulars which may have a bearing upon acceptability have been revealed.

By signing below, the Applicant consents to the Insurer conducting non-intrusive scans of the Applicant's internet-facing systems/applications for common vulnerabilities. It is understood that this application shall form the basis of the contract should the Underwriter approve coverage and the Applicant be satisfied with the Underwriter's quotation. It is further agreed that, if in the time between submission of this application and the requested date for coverage to be effective, the Applicant becomes aware of any information that would change the answers furnished in response to any question of this application, such information shall be revealed immediately in writing to the Underwriter. This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

APPLICANT'S NAME:	TITLE:
SIGNATURE:	DATE:



# FUSION

## Cyber Insurance Application

### NOTICE TO APPLICANT

The insurance for which you are applying will not respond to incidents about which any person proposed for coverage had knowledge prior to the policy's effective date, nor will coverage apply to any claim or circumstance identified or that should have been identified in the loss history questions of this application.

Fraud Warning Language:

Alabama	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 insurance application is guilty of a crime and may be subject to restitution, fines, confinement in prison, or any combination thereof.
Alaska	Any person who knowingly and with intent to injure, defraud, or deceive an insurance company files a claim containing false, incomplete, or misleading information may be prosecuted under state law.
Arizona	For your protection Arizona law requires the following statement to appear on this form: any person who knowingly presents a false or fraudulent claim for payment of a loss is subject to criminal and civil penalties.
Arkansas	Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an insurance application is guilty of a crime and may be subject to fines and confinement in prison.
California	Any person who knowingly presents a false or fraudulent claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.
Colorado	It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company to defraud or attempt 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 to defraud or attempt to defraud the policyholder or claimant about a settlement

# FUSION

## Cyber Insurance Application

	or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.
Delaware	Any person who knowingly, and with the intent to injure, defraud, or deceive any insurer, files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony.
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.
Idaho	Any person who knowingly, with intent to defraud or deceive any insurance company, files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony.
Indiana	A person who knowingly and with the intent to defraud an insurer file a statement of claim containing any false, incomplete, or misleading information commits a felony.
Kentucky	Any person who knowingly and with intent to defraud any insurance company or other person files a statement of claim containing any materially false information or conceals, for misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.
Louisiana	Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an insurance application is guilty of a crime and may be subject to fines and confinement in prison.
Maine	It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties may include imprisonment, fines, or a denial of insurance benefits.
Maryland	Any person who knowingly and willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly and willfully presents false information in an insurance application is guilty of a crime. They may be subject to fines and confinement in prison.
Minnesota	A person who files a claim intending to defraud or helps commit fraud against an insurer is guilty of a crime.

# FUSION

## Cyber Insurance Application

New Hampshire	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.
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.
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 insurance application is guilty of a crime and may be subject to civil fines and criminal penalties.
Ohio	Anyone who intends to defraud or knows that he is facilitating fraud against an insurer applies or files a claim containing a false or deceptive statement is guilty of insurance fraud.
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.
Oregon	Any person who knowingly and with intent to defraud or solicit another to defraud an insurer (1) by applying or (2) by filing a claim containing a false statement as to any material fact to it may be committing a fraudulent insurance act, which may be a crime and may subject the person to criminal and civil penalties.
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 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.
Rhode Island	Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an insurance application is guilty of a crime and may be subject to fines and confinement in prison.
Tennessee	It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.

# FUSION

## Cyber Insurance Application

Texas	Any person who knowingly presents a false or fraudulent claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.
Utah	Any person who knowingly presents false or fraudulent underwriting information, files or causes to be filed a false or fraudulent claim for disability compensation or medical benefits, or submits a false or fraudulent report or billing for health care fees or other professional services is guilty of a crime and may be subject to fines and confinement in state prison. Utah worker's compensation claims only.
Virginia	It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.
Washington	It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties may include imprisonment, fines, or denial of insurance benefits.
West Virginia	Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an insurance application is guilty of a crime and may be subject to fines and confinement in prison.
All Other States	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 insurance application is guilty of a crime and may be subject to restitution, fines, confinement in prison, or any combination thereof.

The Applicant hereby acknowledges that he/she/it is aware that the limit of liability shall be reduced, and may be completely exhausted, by claim expenses and, in such an event, the Insurer shall not be liable for claim expenses or any judgment or settlement that exceed the limit of liability. I HEREBY DECLARE that, after inquiry, the above statements and particulars are true, and I have not suppressed or misstated any material fact. I also agree that this application shall be the basis of the contract with the Underwriters.