☐ **Markel Insurance Company**
☐ **Markel American Insurance Company**
☐ **Evanston Insurance Company**

Markel Cyber 360[SM] Insurance Application

All questions MUST be completed in full.

If space is insufficient to answer any question fully, attach a separate sheet.

Full Name Of Applicant: _____ Title: _____

Business Name: _____

Phone #: _____ Fax #: _____ Email: _____

Mailing Address: _____ City: _____ State: ____ Zip Code: _____

Primary Business Address: _____ City: _____ State: ____ Zip Code: _____

Website: _____

Contact Person & Phone Number: _____

Year Established: _____ NAICS: _____

☐ Individual ☐ Partnership ☐ Corporation ☐ For Profit ☐ Not For Profit ☐ Other _____

1. APPLICANT OPERATIONS

Describe in detail the applicant's business operations:

_____

_____

_____

2. EXPOSURE SUMMARY

a. Please complete the following information for the applicant:

	Most Recent Fiscal Year	Projection For Current Year
Number of employees:		
Total revenue:	$	$
Revenue from e-commerce:	$	$
Number of credit card transactions:		
Number of private data records:		
Number of servers:		
Number of desktops or workstations:		
Number of portable devices:		
Number of office locations:		

b. Does the applicant handle the following types of private data? If yes, provide approximate number of records transmitted, received and stored annually:

	Type Handled?	Number Transmitted	Number Received	Number Stored
Credit or debit cards?	☐ Yes ☐ No			
Financial or banking information?	☐ Yes ☐ No			
Medical information (PHI)?	☐ Yes ☐ No			
Biometric data?	☐ Yes ☐ No			
Geolocation data?	☐ Yes ☐ No			
Social Security Numbers/National Identification Numbers?	☐ Yes ☐ No			
Other private data? (Describe)	☐ Yes ☐ No			
Total				

c. How long does the applicant retain private data? _____

What is the largest number of private data records that the applicant holds at any one time? _____

Describe the method used to dispose of private data: _____

Is the applicant compliant with all federal or state laws with regard to private data transmission, storage, and disposal? ☐ Yes ☐ No

If no, please explain: _____

d. Does the applicant encrypt private data? ☐ Yes, at all times ☐ No ☐ Partially (Describe) _____

If yes, describe encryption method used: _____

3. **POLICIES AND PROCEDURES**

a. Does the applicant use internal staff to manage its IT systems? ☐ Yes ☐ No

b. Does the applicant have a dedicated internal senior manager responsible for information security and privacy? ☐ Yes ☐ No

c. Describe the IT infrastructure the applicant has in place?

_____

What is the amount of the budget the applicant invests in its IT infrastructure? $_____

Does the applicant anticipate either an increase or reduction within the next 12 months? ☐ Yes ☐ No

What does the applicant do to ensure its IT infrastructure is up-to-date?

_____

d. Does the applicant have any significant upgrades, overhauls, or system changes planned in the next 12 months? ☐ Yes ☐ No

If yes, describe: _____

Does a roll back plan exist if migration cannot be completed? ☐ Yes ☐ No

Will extensive testing be completed prior to launch? ☐ Yes ☐ No

e. Identify the type of software deployed by the applicant in the normal course of its operations and describe the primary function of the software: _____

f. Does the applicant have written information security policies and procedures that are reviewed annually? ☐ Yes ☐ No

g. Does the applicant require information security awareness training for all staff at least annually? ☐ Yes ☐ No

h. Does the applicant have a security patch management process implemented? ☐ Yes ☐ No

If yes, how are security patch notifications from its major systems vendors handled?

☐ Manual notice (describe): _____

☐ Automatic notice (where available) and implemented in more than 30 days

☐ Automatic notice (where available) and implemented in 30 days or less

i. Which of the following procedures does the applicant use to test computer security controls?

Test	**Frequency Of Testing**
Internal vulnerability scanning:	☐ Continuous ☐ Monthly ☐ Quarterly
External vulnerability scanning against internet-facing IP addresses:	☐ Continuous ☐ Monthly ☐ Quarterly
Penetration testing:	☐ Quarterly ☐ Bi-Annually ☐ Annually
Other (describe):	

j. Does the applicant have a/an:

Business continuity plan?	☐ Yes – Date Last Tested:	☐ No
Disaster recovery plan?	☐ Yes – Date Last Tested:	☐ No
Incident response plan for network intrusions and virus incidents?	☐ Yes – Date Last Tested:	☐ No

Briefly describe the plan(s): _____

Are alternative facilities available for operations in the event of a shutdown or failure of the applicant's network? ☐ Yes ☐ No

Does the business continuity plan contemplate disruptions due to outsourced service providers? ☐ Yes ☐ No

If yes, is it tested? ☐ Yes ☐ No

Does the plan consist of multiple outsourced service providers in place for the same services? ☐ Yes ☐ No

k. Does the applicant have a written policy regarding setting up electronic funds transfer? ☐ Yes ☐ No

If yes, is the policy communicated to all applicable associates? ☐ Yes ☐ No

Are all fund transfers subject to dual authentication, including confirmation by phone of the wire transfer instruction? ☐ Yes ☐ No

What is the average number of funds transfers per day? _____

What is the average value of funds transfers? $_____

l. Is the applicant certified as complying with the following security requirements:

(1) Payment Card Industry (PCI/DSS)? ☐ N/A ☐ Yes ☐ No ☐ In Progress - Scheduled Date: _____

If yes, provide the name of the individual or outside organization which certified the applicant and the date of the last PCI audit.

_____

(2) HIPAA/HITECH? ☐ N/A ☐ Yes ☐ No ☐ In Progress - Scheduled Date: _____

4. **NETWORK AND TECHNOLOGY PROVIDERS**

a. Please identify the current provider for each of the following:

Anti-virus software:	Internet communications services:
Broadband ASP services:	Intrusion detection software:
Cloud services:	Managed security services:
Collocation services:	Outsourcing services:
Credit card processors:	Website hosting:
Firewall technology:	Other (describe):

b. Complete the following for cloud services used by the applicant for processing or storing private data:

Cloud Provider	Type	Service	# Of Records	Encrypted Storage
				☐ Yes ☐ No
				☐ Yes ☐ No

c. How frequently are internal/external audit reviews performed on the applicant's network? _____

Who performs the audit reviews? _____

5. **CONTINGENT BUSINESS INTERRUPTION**

a. Does the applicant contractually require that all outsourced service providers carry cyber insurance? ☐ Yes ☐ No

If yes, what limits are required? $_____

Does the applicant receive contractual indemnification agreements from its outsourced service providers regarding their cyber business interruption exposure? ☐ Yes ☐ No

Does the applicant receive service level agreements such as 99% uptime guarantees? ☐ Yes ☐ No

b. Does the applicant currently use any outsourced service provider that has had a known cyber event or system failure? ☐ Yes ☐ No

c. Explain the applicant's screening process of its outsourced service providers (e.g. IT security audits, questionnaires):

_____

d. Does the applicant perform reviews at least annually of the outsourced service providers to ensure they adhere to the applicant's requirements for data protection? ☐ Yes ☐ No

6. **ACCESS CONTROL**

a. How does the applicant limit access to its IT systems?

☐ Unique user IDs ☐ Unique user IDs and role based access to private data ☐ Multifactor authentication

b. Does the applicant delete access to its IT systems after employee termination? ☐ Yes ☐ No

c. Is access to equipment, such as servers, workstations, and storage media including paper records, containing private data physically protected? ☐ Yes ☐ No

d. Does the applicant have anti-virus, anti-spyware, and anti-malware software installed? ☐ Yes ☐ No

If yes, check all that apply:

☐ On all desktop and laptop computers with automatic updates	☐ Scanning of all incoming email
☐ On all server computers with automatic updates	☐ Scanning of all web browsing

e. Does the applicant implement firewalls and other security measures between the internet and private data? ☐ Yes ☐ No

f. Are security alerts from an intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored and are the latest IDS/IPS signatures installed regularly? ☐ Yes ☐ No

g. Is remote access to the applicant's IT systems restricted to VPN or equivalent? ☐ Yes ☐ No

h. Does the applicant have wireless networks deployed? ☐ Yes ☐ No

If yes, are all wireless access points to the applicant's network encrypted with market standard encryption (e.g. WPA/WPA2)? ☐ Yes ☐ No

Is there a firewall between all wireless access points and the parts of the applicant's network on which private data is stored? ☐ Yes ☐ No

7. **DATA PROTECTION**

a. Does the applicant store private data on any of the following media? If yes, is it encrypted?

	Private Data	**Encrypted**
Laptop or notebook computers:	☐ Yes ☐ No	☐ Yes ☐ No
Other mobile devices:	☐ Yes ☐ No	☐ Yes ☐ No
Flash drives or other portable storage devices:	☐ Yes ☐ No	☐ Yes ☐ No
Backup tapes:	☐ Yes ☐ No	☐ Yes ☐ No
Internet connected web servers:	☐ Yes ☐ No	☐ Yes ☐ No
Databases, audit logs, files on servers:	☐ Yes ☐ No	☐ Yes ☐ No
Email:	☐ Yes ☐ No	☐ Yes ☐ No

b. Where private data is stored but not encrypted, please detail what other measures to protect private data are in place:

_____

c. How often are back-ups of the applicant's systems performed? _____

d. How quickly could the applicant's systems be restored from back-ups? _____

e. Are key data and software code stored:

On a secondary storage device? ☐ Yes ☐ No

At a secured offsite storage? ☐ Yes ☐ No

Utilizing a cloud storage service? ☐ Yes ☐ No

8. **MEDIA OFFENSE LIABILITY**

a. Does the applicant send any electronic advertising content to outside parties regarding its products or services, or the products or services of it clients? ☐ Yes ☐ No

If yes, which media does the applicant use? ☐ SMS Text Messaging ☐ Phone Calls ☐ Email ☐ Other (describe): _____

b. Does the applicant conduct prior review of any content for copyright or trademark infringement, libel or slander, and violation of rights of privacy or publicity? ☐ Yes ☐ No

c. Which of the following types of content or information is available on the applicant's website:

☐ Adult content	☐ Educational	☐ News
☐ Advertisements	☐ Entertainment	☐ Product comparison
☐ Children	☐ Games/Quizzes	☐ Rating/Grading
☐ Culture	☐ How-to	☐ Referral services
☐ Digital music	☐ Information/E-brochure	☐ Sports
☐ Downloadable software	☐ Medical	☐ Other (describe):

d. Does the applicant collect data about children who use its website? ☐ Yes ☐ No

If yes, does the applicant obtain parental consent regarding its collection of such data? ☐ Yes ☐ No

e. Describe the take down procedures when notified that content is defamatory, infringing, or in violation of a third party's privacy rights or otherwise improper:

f. Does the applicant obtain clear rights to intellectual property (IP) supplied by third parties if such IP is displayed on its website? ☐ Yes ☐ No

g. Does the applicant utilize hyperlinks or allow for data scraping on its website? ☐ Yes ☐ No

h. Does the applicant use the names or likeness of any celebrities or other public figures on its website? ☐ Yes ☐ No

9. OTHER INSURANCE AND LOSS HISTORY

a. List current and prior cyber liability or cyber security insurance for each of the last 3 years:

If none, check here ☐

Insurance Company	Limits Of Insurance	Deductible	Premium	Inception And Expirations Dates (MM/DD/YYYY)	Retroactive Or Prior Acts Date (MM/DD/YYYY)
	$	$	$		
	$	$	$		
	$	$	$		

b. Provide the following information:

	Insurer	Limit	Deductible	Expiration Date (MM/DD/YYYY)
General Liability		$	$	
Professional Liability		$	$	

c. Is the applicant aware of any loss, claim, suit, incident or notice of incident against the applicant, its predecessors in business, any of the present or past partners, officers, employees, or any other individual who would fall under coverage proposed, or has any claim, suit, incident or notice of incident been made against the applicant or any staff member? ☐ Yes ☐ No

If yes, please provide full details:

d. Is the applicant aware of any facts, circumstances, incidents, situations, or data compromise which may result in any loss, claim, suit, or incident against the applicant, its predecessors in business, any of the present or past partners, officers, employees, or any individual who would fall under coverage proposed? ☐ Yes ☐ No

If yes, please provide full details:

Please provide any additional information the applicant believes could be important for the Company to consider prior to making a coverage determination.

Fair Credit Report Act Notice

Personal information about you, including information from a credit or other investigative report, may be collected from persons other than you in connection with this application for insurance and subsequent amendments and renewals. Such information as well as other personal and privileged information collected by us or our agents may in certain circumstances be disclosed to third parties without your authorization. Credit scoring information may be used to help determine either your eligibility for insurance or the premium you will be charged. We may use a third party in connection with the development of your score. You have the right to review your personal information in our files and can request correction of any inaccuracies. A more detailed description of your rights and our practices regarding such information is available upon request. Contact your agent or broker for instructions on how to submit a request to us.

Fraud Warnings

Applicable in AL, AR, DC, LA, MD, NM, RI and WV: 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. *Applies in MD only.

Applicable in CO: 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 FL and OK: 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)*. *Applies in FL only.

Applicable in KS: 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 commits a fraudulent insurance act.

Applicable in KY, NY, OH and PA: 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 (not to exceed five thousand dollars and the stated value of the claim for each such violation)*. *Applies in NY only.

Applicable in ME, TN, VA and WA: 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 and denial of insurance benefits. *Applies in ME only.

Applicable in MN: A person who files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

Applicable in NJ: 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 OR: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact may be violating state law.

Applicable in VT: 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 all other states: 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 THE APPLICANT - PLEASE READ CAREFULLY

NO FACT, CIRCUMSTANCE, OR SITUATION INDICATING THE PROBABILITY OF A CLAIM OR ACTION FOR WHICH COVERAGE MAY BE AFFORDED BY THE PROPOSED INSURANCE IS NOW KNOWN BY ANY PERSON(S) OR ENTITY(IES) PROPOSED FOR THIS INSURANCE OTHER THAN THAT WHICH IS DISCLOSED IN THIS APPLICATION. IT IS AGREED BY ALL CONCERNED THAT IF THERE IS KNOWLEDGE OF ANY SUCH FACT, CIRCUMSTANCE, OR SITUATION, ANY CLAIM SUBSEQUENTLY EMANATING THEREFROM WILL BE EXCLUDED FROM COVERAGE UNDER THE PROPOSED INSURANCE.

FOR THE PURPOSE OF THIS APPLICATION, THE UNDERSIGNED AUTHORIZED AGENT OF THE PERSON(S) AND ENTITY(IES) PROPOSED FOR THIS INSURANCE DECLARES THAT TO THE BEST OF HIS OR HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS IN THIS APPLICATION AND IN ANY ATTACHMENTS ARE TRUE AND COMPLETE. THE COMPANY AND AFFILIATES THEREOF ARE AUTHORIZED TO MAKE ANY INQUIRY IN CONNECTION WITH THIS APPLICATION. SIGNING THIS APPLICATION DOES NOT BIND THE COMPANY TO PROVIDE OR THE APPLICANT TO PURCHASE THE INSURANCE.

THIS APPLICATION, INFORMATION SUBMITTED WITH THIS APPLICATION AND ALL PREVIOUS APPLICATIONS AND MATERIAL CHANGES THERETO ARE CONSIDERED PHYSICALLY ATTACHED TO AND PART OF THE POLICY IF ISSUED. THE COMPANY WILL HAVE RELIED UPON THIS APPLICATION AND ALL SUCH ATTACHMENTS IN ISSUING THE POLICY.

IF THE INFORMATION IN THIS APPLICATION AND ANY ATTACHMENT MATERIALLY CHANGES BETWEEN THE DATE THIS APPLICATION IS SIGNED AND THE EFFECTIVE DATE OF THE POLICY, THE APPLICANT WILL PROMPTLY NOTIFY THE COMPANY, WHO MAY MODIFY OR WITHDRAW ANY OUTSTANDING QUOTATION OR AGREEMENT TO BIND COVERAGE.

THE UNDERSIGNED DECLARES THAT THE PERSON(S) AND ENTITY(IES) PROPOSED FOR THIS INSURANCE UNDERSTAND THAT:

(I) THE POLICY FOR WHICH THIS APPLICATION IS MADE APPLIES ONLY TO CLAIMS FIRST MADE DURING THE POLICY PERIOD;

(II) UNLESS AMENDED BY ENDORSEMENT, THE LIMITS OF INSURANCE CONTAINED IN THE POLICY WILL BE REDUCED, AND MAY BE COMPLETELY EXHAUSTED BY CLAIM EXPENSES AND, IN SUCH EVENT, THE COMPANY WILL NOT BE LIABLE FOR CLAIM EXPENSES OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT TO THE EXTENT THAT SUCH COSTS EXCEED THE LIMITS OF INSURANCE IN THE POLICY; AND

(III) UNLESS AMENDED BY ENDORSEMENT, CLAIM EXPENSES WILL BE APPLIED AGAINST THE RETENTION.

WARRANTY

The undersigned warrants to the Company that he/she understands and accepts the notice stated above and that the information contained herein is true and will be the basis of the policy and deemed incorporated therein, should the Company evidence its acceptance of this application by issuance of a policy. The undersigned authorize the release of claim information from any prior insurer to the Company or affiliates thereof.

This application is signed by undersigned authorized agent of the applicant(s) on behalf of the applicant(s) and its owners, partners, directors, officers, and employees.

This application must be signed by the owner, principal, partner, executive officer, or equivalent within 60 days of the proposed effective date.

Name of applicant	Title
Signature of applicant	Date

(Florida only) Agent license number: _____

☐ **Markel Insurance Company**
☐ **Markel American Insurance Company**
☐ **Evanston Insurance Company**

Markel Cyber 360[SM] Supplemental Application For Ransomware

All questions MUST be completed in full.

If space is insufficient to answer any question fully, attach a separate sheet.

Full Name of Insured: _____

Business Name: _____

1. Does the Insured authenticate inbound email using tools such as DMARC (Domain-based Message Authentication Reporting, and Conformance)?	☐ Yes	☐ No
2. Does the Insured scan and filter inbound emails for malicious content (such as executable files)?	☐ Yes	☐ No
3. Does the Insured train users against phishing and social engineering threats via ongoing campaigns and assessments?	☐ Yes	☐ No
4. Does the Insured's response plan reference mitigation steps for business continuity and recovery should a ransomware incident occur?	☐ Yes	☐ No
5. Does the Insured make regular backups of critical data?	☐ Yes	☐ No
6. Does the Insured keep backups offline and segmented from the Insured's network?	☐ Yes	☐ No
7. Is the integrity of the backups and recovery plans regularly tested?	☐ Yes	☐ No
8. Does the Insured enforce a BYOD (Bring Your Own Device) policy that ensures critical data is encrypted when transferred to portable media devices (USBs, laptops, etc.)?	☐ Yes	☐ No

If NO to any of the above, please detail below along with mitigating comments:

NOTE: This Supplement becomes part of the primary application and must be signed and dated. Coverage cannot be bound until the Company approves the completed application. The Company's receipt of premium does not bind coverage until a written quote has been issued.

_____ _____
Name of applicant Title

_____ _____
Signature of applicant Date

(Florida only) Agent license number: _____

☐ Evanston Insurance Company
☐ Markel American Insurance Company
☐ Markel Insurance Company

Contingent Business Interruption And System Failure Supplement

All questions MUST be completed in full.

If space is insufficient to answer any question fully, attach a separate sheet.

Full Name Of Applicant: _____ Title: _____

Business Name: _____

Section I Contingent Business Interruption

1. Does the applicant contractually require their outsourced service providers to carry Data Breach insurance and at what limit? _____

   _____

2. Does the applicant receive contractual indemnification agreements from their outsourced service providers regarding their Data Breach Business Interruption exposure? Do they receive service level agreements such as 99% uptime guarantees? _____

   _____

3. Please explain the applicants screening process of their outsourced service providers (ex. IT security audits, questionnaires). _____

   _____

4. Does the applicant have multiple outsourced service providers in place for the same service in the event one fails?

   _____

   _____

5. Does the applicant have a Business Continuity Plan in place that contemplates disruptions due to outsourced service providers and is it tested? _____

   _____

6. Does the applicant maintain a risk register that includes their top outsourced service providers in order to mitigate issues? _____

   _____

7. Does the applicant currently use an outsourced service provider that has had a known cyber event? _____

   _____

   _____

8. In the table below please list your top 5 outsourced service providers and their function.

Outsourced Service Provider	Service Provided (function)

Section II System Failure

1. a. Does the applicant have any significant upgrades, overhauls or system changes planned in the next 12 months?

   _____

   _____

   b. If so, does a roll back plan exist if migration cannot be completed and will extensive testing be completed prior to launch? _____

   _____

2. Please identify the type of software deployed by the applicant in the normal course of its operations and describe the primary function of that software. _____

   _____

   _____

3. What is the applicant's investment in its IT infrastructure and what has been done to ensure it is up to date?

   _____

   _____

4. What is the structure of the applicant's IT management department and how long have they been in place?

   _____

   _____

5. Does the applicant have a Business Continuity Plan in place that contemplates disruptions due to system failures and is it tested? _____

   _____

Section III Additional Measures

Please provide any other applicable comments or information below, if necessary. _____

_____

_____

_____

_____

_____

Signing this supplemental application does not bind the Company to provide or the applicant to purchase the insurance.

It is understood that information submitted herein becomes a part of our application for insurance and is subject to the same declarations, representations and conditions.

This supplemental must be signed by a director, executive officer, partner or equivalent within 60 days of the proposed effective date.

_____	_____
Name of Applicant	Title
_____	_____
Applicant's signature	Date