Markel Cyber 360™ Insurance Supplemental Application

[ ] **Markel American Insurance Company**
[ ] **Evanston Insurance Company**

All questions MUST be completed in full. If space is insufficient to answer any question fully, attach a separate sheet.

Full Business Name of Applicant: _____

Website: _____

Primary Business Address: _____

City: _____ State: _____ Zip Code: _____

Information Security Contact Person: _____ E-Mail Address: _____

Phone Number: _____

[ ] IT Director [ ] Director/Manager of Security Operations [ ] Director/Manager of IT Security [ ] Security Analyst

[ ] Information Security Director/Manager [ ] Other: _____

General information:

Describe in detail the Applicant's business operations:

1. a. Please complete the following information for the Applicant:

	Most Recent Fiscal Year	Projection For Current Year	Next Year (Estimate)
Total revenue:	$	$	$
US revenue:	$	$	$
Foreign revenue:	$	$	$
Number of employees:			
Number of endpoints:			

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

	Type Handled?	Number Transmitted	Number Received	Number Stored
Payment card information?	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 (PII)? (Describe)	Yes [ ] No [ ]			
Total				

2. Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? ..... Yes [ ] No [ ]

3. Please indicate the Applicant's four largest customer engagements for the past 2 years:

Client:		Client:	
Product / Service:		Product / Service:	
Revenues		Revenues	
Client:		Client:	
Product / Service:		Product / Service:	
Revenues		Revenues	

4. Does the Applicant have written contracts for all service / product engagements with all customers?..... Yes [ ] No [ ]

   If 'No', what percentage of the time are written contracts used? _____%

Data Privacy

1. Has the Applicant designated a:

   - Chief Privacy Officer? ..... Yes [ ] No [ ]

   If 'No', please indicate what position is responsible for compliance with privacy regulations: _____

2. Does the Applicant have a documented company-wide Privacy Policy? ..... Yes [ ] No [ ]

   How often is the Policy reviewed? _____

3. Is the Applicant compliant with all applicable international, federal and/or state laws with regard to data transmission, storage, and disposal? ..... Yes [ ] No [ ]

   If 'No', please describe:_____

4. Which of the following are used to verify compliance with privacy regulations and notification?

   - Internal counsel ..... Yes [ ] No [ ]
   - Outside counsel ..... Yes [ ] No [ ]
   - Automated privacy management software tool ..... Yes [ ] No [ ]
     - o Which product(s) are used?: _____

5. Does the Applicant have a process in place to allow customers to Opt in/Opt out of communications? ..... Yes [ ] No [ ]

Controls:

Access Controls

1. Has the Applicant designated a:

   - Chief Information Security Officer (as respects computer systems and data security)?: ..... Yes [ ] No [ ]

     If 'No', please indicate what position if responsible for computer and data security: _____

2. Does the Applicant require Multi-Factor Authentication for:

   - Privileged User accounts? ..... Yes [ ] No [ ]
   - All Cloud resources including Office365? ..... Yes [ ] No [ ]
   - All Third-Parties/Vendors & Contractors? ..... Yes [ ] No [ ]

3. Does all remote access to the Applicant's network and corporate email, including web applications, require multifactor authentication (MFA)? ..... Yes [ ] No [ ]
4. Does the Applicant allow local admin rights on workstations? ..... Yes [ ] No [ ]
5. Has the Applicant disabled remote desktop protocol (RDP)? ..... Yes [ ] No [ ]

   If 'No', has the Applicant implemented the following: [ ] VPN [ ] MFA [ ] RDP Honeypots
6. Do administrative/privileged accounts use a privilege access management (PAM) tool? ..... Yes [ ] No [ ]

   Which product(s) are used?: _____
7. Is the applicant deploying a Zero Trust security framework requiring all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration before being granted or maintain access to application and data? ..... Yes [ ] No [ ]
8. Is the applicant using the following features of a Zero Trust security framework, whether inside or outside the organization's network?
   - Geo Fencing (by device, location, etc.) ..... Yes [ ] No [ ]
   - MFA ..... Yes [ ] No [ ]
   - Conditional Access ..... Yes [ ] No [ ]
   - Risk based Access Controls ..... Yes [ ] No [ ]
   - Access Controls for SaaS application (i.e. CASB) ..... Yes [ ] No [ ]

Internal Security

1. Does the Applicant use an Endpoint Detection and Response (EDR) tool? _____ Yes [ ] No [ ]

   If 'Yes':
   - Please indicate which product(s) _____
   - Does the EDR have AI/automated enforcement enabled? ..... Yes [ ] No [ ]

     If 'Yes', is it: [ ] Rules based [ ] Behavioral [ ] No automated enforcement
   - Please indicate the percentage of the Applicant's system that is visible to the EDR tool(s):

     • Servers: _____ Endpoints: _____
2. Does the Applicant use an endpoint protection (EPP) tool? ..... Yes [ ] No [ ]

   If 'Yes', which product(s): _____
3. Does the Applicant use a data loss prevention (DLP) tool? ..... Yes [ ] No [ ]

   If 'Yes', which product(s): _____
4. Does the Applicant use O365 in your organization?

   [ ] Yes. Have the following been implemented? [ ] MFA [ ] ATP [ ] Macros disabled by default

   [ ] No. Which products are used for email monitoring (e.g. Proofpoint)? _____
5. Does the Applicant operate a SIEM monitored by:

   [ ] Dedicated SOC/MSSP (internal/external staff – on call rotations 24x7)

   [ ] Dedicated SOC/MSSP (internal/external staff – on call rotations 9x5)

   [ ] Internal IT Staff Receives Email 24x7

   [ ] Internal IT Staff Receives Emails, Only Responding When on the Clock

   [ ] No Monitoring

6. In what time frame does the Applicant install critical and high severity patches?

   [ ] Within 2 weeks [ ] Within 1 month [ ] Within 2 months [ ] Other, please describe: _____

7. If the Applicant has any end of life or end of support software, is it segregated from the rest of the network? ..... Yes [ ] No [ ] Partial [ ] N/A [ ]

8. What is the Applicant's RTO for critical business systems?

   [ ] less than 8 hours [ ] 8-12 hours [ ] 12-18 hours [ ] greater than 18 hours

9. Does the Applicant have a written:

   - Business Continuity Plan?

     Yes [ ] No [ ] Date Last Tested: _____

   - Disaster Recovery Plan?

     Yes [ ] No [ ] Date Last Tested: _____

   - Incident Response Plan?

     Yes [ ] No [ ] Date Last Tested: _____

   - Incident response plan for network intrusions and virus incidents?

     Yes [ ] No [ ] Date Last Tested: _____

Briefly describe the plan(s):

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

11. Does the business continuity plan contemplate disruptions due to outsourced service providers? ..... Yes [ ] No [ ]

    a. **If 'Yes',** is it tested? ..... Yes [ ] No [ ]

12. Does the plan require multiple/redundant outsourced service providers in place for the same services? ..... Yes [ ] No [ ]

13. Does the Applicant's incident response plan (IRP) specifically address ransomware scenarios? ..... Yes [ ] No [ ]

    - When was the date of last IRP with Ransomware exercise? _____

Please outline any additional controls the Applicant's organization has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, DNS, network segmentation, vulnerability scanning, phishing training):

14. What is the largest number of records that the Applicant holds in one segment? _____

    - Are you deploying: [ ] Segmentation or [ ] Micro-Segmentation [ ] None of sensitive data?

15. Do you encrypt data: 1) In transit Yes [ ] No [ ] 2) At Rest Yes [ ] No [ ] 3) On Mobile Devices Yes [ ] No [ ]

    If 'No' to any of the above, please describe: _____

16. Do you apply a least privilege access model to sensitive data? ..... Yes [ ] No [ ]

    Please describe: _____

Email Security

1. Does the Applicant authenticate emails using: [ ] SPF [ ] DKIM and/or [ ] DMARC
2. Does the Applicant have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end user? ..... Yes [ ] No [ ]
3. Are external emails flagged? ..... Yes [ ] No [ ]

Backup, Recovery & Data Protection

1. How frequently does the Applicant back up critical data? [ ] Daily [ ] Weekly [ ] Monthly [ ] Other
2. Which of the following are used to store backups?

   [ ] Cloud Storage [ ] Secondary Data Center [ ] Offline Storage within a separate network segment
3. Does the Applicant's backup strategy include the following?
   - Segmentation ..... Yes [ ] No [ ]
   - Encryption ..... Yes [ ] No [ ]
   - MFA ..... Yes [ ] No [ ]
   - Vaulted Credentials ..... Yes [ ] No [ ]
   - Tested for Restore ..... Yes [ ] No [ ]
   - Immutable ..... Yes [ ] No [ ]
   - Scanned for Malware ..... Yes [ ] No [ ]

   If **'No'** to any of the above, please describe below along with compensation controls:

Supply Chain & Third-Party / Vendor Management

1. Please list the three largest technology vendors for critical business processes:

   1. _____ 2. _____ 3. _____
2. Does the Applicant have a formal written third-party/vendor management policy in place that specifically addresses data security and ransomware? ..... Yes [ ] No [ ]
3. Are contracts required of all third-parties/vendors? ..... Yes [ ] No [ ]

   If **so**:
   - Does the Applicant require third-parties with which it shares personally identifiable or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? ..... Yes [ ] No [ ]
   - What percentage of the time are such contracts executed?

     [ ] 0-25% [ ] 26%-50% [ ] 51%-75% [ ] 76%-100%
4. Does the Applicant require that third-parties/vendors carry Cyber Security Insurance? ..... Yes [ ] No [ ]
5. Does the Applicant conduct routine audits of third-parties/vendors? ..... Yes [ ] No [ ]
   How often? [ ] Quarterly [ ] Annually [ ] Bi-Annuall [ ] Other

   Who performs the audit reviews? _____
6. Does least privilege apply to third-party/vendor access to the Applicant's network? ..... Yes [ ] No [ ]
7. Is dual authorization required for all wire transfers? ..... Yes [ ] No [ ]
8. Are all changes requested by the vendor (including bank account, invoice changes, telephone or FAX numbers, address and other contact information) verified by the Applicant by a direct call to the vendor using only the telephone number provided by the vendor before the request is received? ..... Yes [ ] No [ ]

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

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

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

Cloud Provider	Type	Service	# Of Records	Encrypted Storage
				Yes [ ] No [ ]
				Yes [ ] No [ ]

Employee Training

1. How often are phishing campaigns conducted?

   [ ] Never [ ] Monthly [ ] Quarterly [ ] Annually [ ] Ad Hoc

2. How often is security awareness training conducted for all staff?

   [ ] Never [ ] Monthly [ ] Quarterly [ ] Annually [ ] Ad Hoc

   • Is Fraudulent Impersonation training included in security awareness training? ..... Yes [ ] No [ ]

3. How often is phishing specific cybersecurity training conducted for elevated access users?

   [ ] Never [ ] Monthly [ ] Quarterly [ ] Annually [ ] Ad Hoc

Payment Cards – PCI / DSS

1. Is the Applicant PCI compliant? ..... Yes [ ] No [ ]
   - If so, what level and when was compliance achieved? Level: _____ Date: _____
2. Is segmentation used to isolate PCI information from the rest of the corporate network? ..... Yes [ ] No [ ]
3. Does the Applicant use a third-party vendor for e-commerce payment processing? ..... Yes [ ] No [ ]

   If **'Yes'**, please provide the vendor: _____
4. Is payment card data stored on the Applicant's network? ..... Yes [ ] No [ ]
   - If **'Yes'**, is it encrypted At Rest and In Transit? ..... Yes [ ] No [ ]
   - If **'Yes'**, do you apply a privileged access management security (PAM) tool for access? ..... Yes [ ] No [ ]
5. Is payment card data encrypted at the point of sale (e.g., payment card reader or e-commerce payment portal) through transmission to the payment processor? ..... Yes [ ] No [ ]
6. Is tokenization used to remove the actual credit card number from the transaction? ..... Yes [ ] No [ ]

   If **'Yes'**, please provide the vendor: _____
7. Do you have installed, maintained, and regularly updated firewall configuration and antivirus software to protect cardholder data? ..... Yes [ ] No [ ]

Media

1. Does the Applicant use a 3rd party marketing or advertising agency? ..... Yes [ ] No [ ]
2. Does the Applicant provide any services to third parties related to media operations for a fee, (i.e. advertising or printing services, etc.)? ..... Yes [ ] No [ ]
3. Are staff members with responsibility for content trained with respect to defamation, invasion of privacy, intellectual property and other exposures? ..... Yes [ ] No [ ]
4. Is any user-generated content uploaded to your website(s)? ..... Yes [ ] No [ ]
   - **If 'Yes'**, please answer the following: Does the Applicant review content? ..... Yes [ ] No [ ]
5. Is the name, likeness, or portrayal of any real person, private location, audio recording or trademark used in any content? ..... Yes [ ] No [ ]
   - **If 'Yes',** are all intellectual property clearances obtained? ..... Yes [ ] No [ ]

Other Insurance and Loss History

1. 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)
	$	$	$		
	$	$	$		
	$	$	$		
	$	$	$		
	$	$	$		

2. Provide the following information:

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

3. Is the Applicant aware of any loss, claim, suit, incident or notice of incident, arbitration proceeding, administrative proceeding, regulatory proceeding, or investigation 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:

4. 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.

NOTE: This Supplement becomes part of your primary application and must be signed and dated. Coverage cannot be bound until the Company approves your completed application. The Company's receipt of premium does not bind coverage until a written quote has been issued. Before electronically signing this document, verify your information is correct. Electronically signing will disable further editing of your application.

Name of applicant

Title

Signature of applicant

Date

(Florida only) Agent license number: _____