AXIS CYBER APPLICATION

AXIS INSURANCE
111 S. Wacker Dr., Ste. 3500
Chicago, IL 60606
Telephone**: (678) 746-9000** | Toll-Free**: (866) 259-5435** | Fax: **(678) 746-9315**
https://www.axiscapital.com/insurance/cyber-technology-e-o

SOLELY AS RESPECTS CLAIMS-MADE LIABILITY COVERAGES UNDER THE POLICY FOR WHICH THIS APPLICATION IS BEING SUBMITTED: THIS INSURANCE POLICY PROVIDES COVERAGE ON A CLAIMS-MADE AND REPORTED BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD AND REPORTED TO THE INSURER AS SET FORTH IN THE REPORTING OF CLAIMS AND EVENTS SECTION. DEFENSE COSTS ARE INCLUDED IN THE LIMITS OF INSURANCE, AND PAYMENT THEREOF WILL ERODE, AND MAY EXHAUST, THE LIMITS OF INSURANCE.

NEW BUSINESS APPLICATION

“Applicant" refers individually and collectively to all proposed insureds. All responses shall be deemed made on behalf of all proposed insureds. **If responses differ for any proposed insureds (including subsidiaries) please complete additional supplementals for those**

This Application and all materials submitted herewith shall be held in confidence.

The submission of this Application does not obligate the Applicant to buy insurance nor is the Insurer obligated to sell insurance or to offer insurance upon any specific terms requested.

If the policy applied for is issued, this Application, which shall include all Supplemental Applications and material and information submitted in connection with this Application, will be deemed attached to and will form a part of the policy.

INSTRUCTIONS

Respond to all questions completely, leaving no blanks. Check responses when requested.

If space is insufficient, continue responses in additional commentary box at the end of the Application.

This Application must be completed, dated, and signed by an authorized officer of the entity identified in the section entitled "Applicant Information" below.

APPLICANT INFORMATION

Applicant Name:	

Mailing Address:				
Website(s):				
Risk Manager Contact:				
Incident Response Contact:				
Business Activities:	Please describe the Applicant's business activities, services and products			
Revenue:	Annual gross revenue projected for current fiscal year			
Annual gross revenue for previous fiscal year				
Operating Cost:	Annual operating cost for current fiscal year			
Current fiscal year budget allocation to		IT:	Cybersecurity:	
Headcount:	Employees:		Contractors:	
Working remotely:				
Regions:	Percentage of projected revenue in each region where the applicant operates:			
% US	% Canada	% UK	% Europe	% AUS/NZ
% LATAM	% Russia	% MEA	% APAC	
Ownership Structure:	Category best describing ownership structure: Select all that apply			
☐ Publicly traded	☐ Privately held	☐ Subsidiary	☐ Government	☐ Nonprofit

ASSETS

Personal Information:	For purposes of this application, Personal Information refers to PII, PHI, PCI and Biometric Information described below.	
With respect to each of the following types of Personal Information, what is the approximate number of unique individuals whose Personal Information is collected, stored, used or processed by the Applicant or by a third party on behalf of the applicant?		
PII	Information from which an individual can be uniquely and reliably identified or contacted or that is used for authenticating an individual for business transactions or access to the individual's accounts or records. (Individual's name, address, email address, telephone number, passport, social security, driver's license or other government issued identification numbers, credit, debit or other financial account numbers, security codes, passwords, PINs and security questions and answers)	
PHI	Individual's health or medical information (Individual's name, medical records, medical history, medical bills, lab test results, medical record numbers, health plan or health beneficiary numbers, medical device identifiers and serial numbers)	
PCI	Payment card information	
Biometric	An individual's unique physical or behavioral characteristics. (Fingerprints, faceprints, hand scans, vein patterns, voiceprints, iris or retina scans, keystroke, gait or other physical patterns, sleep/health/exercise data, DNA or biological markers)	
Does the Applicant sell or share Personal Information?		☐ Yes ☐ No
Does the Applicant store or process Personal Information on behalf of a third party?		☐ Yes ☐ No
Corporate Information:	For purposes of this application, Corporate Information refers to third party IP, intangible assets, trade secrets, nonpublic business information, such as insider financial information, M&A and business or product development information, client lists, sales projections and strategy, or information that is marked "confidential".	
Does the Applicant store or process Corporate Information?		☐ Yes ☐ No
Critical Information:	For purposes of this application, Critical Information refers to systems, software, programs, applications and information that are critical to the Applicant's business.	
Please describe any information considered to be Critical Information		

Please describe any extra security measures applied to Critical Information?				
Network:	Does the Applicant's network include the following: Select all that apply			
☐ Web applications	☐ Hosted applications	☐ POS systems	☐ Personal devices	☐ BYOD devices
☐ Terminals (ATMs)	☐ Removable media (USBs, offline storage)	☐ Vehicular onboard systems	☐ Critical IoT (Security, fire, BAS)	☐ OT/ICS/SCADA
☐ Healthcare devices	☐ AI/robotic devices			
Which store or process Protected Personal Information, Corporate Information or Critical Information or execute critical business processes? Select all that apply				
☐ Web applications	☐ Hosted applications	☐ POS systems	☐ Personal devices	☐ BYOD devices
☐ Terminals (ATMs)	☐ Removable media (USBs, offline storage)	☐ Vehicular onboard systems	☐ Critical IoT (Security, fire, BAS)	☐ OT/ICS/SCADA
☐ Healthcare devices	☐ AI/robotic devices			
How many servers are on the Applicant's network?				
Where are the servers located? Select all that apply				
☐ US	☐ Canada	☐ UK	☐ Europe	☐ AUS/NZ
☐ LATAM	☐ Russia	☐ MEA	☐ APAC	
Hardware TIV:	What is the approximate replacement value of the Applicant's desktop and laptop computers and associated input/output devices, mobile devices and networking, data storage, backup and peripheral devices?			

Website:	Is the Applicant's website critical to the Applicant's daily business?		☐ Yes ☐ No
How is the website managed?	☐ In house	☐ Outsourced	
Do contractors or service providers have administrator privileges on the website?			☐ Yes ☐ No
Additional Comments about Assets:			

GOVERNANCE

Information Security Officer:	Identify the most senior role in the company having responsibility for information security, such as CISO (chief information security officer) or CSO (chief security officer) or functional equivalent.	
Does this role have direct responsibility for managing security incident response?		☐ Yes ☐ No
To whom does this role report? Select all that apply	☐ Executive officers or committee of executive officers	
☐ Board of directors	☐ Principal owners or shareholders	
Identify any other		
How frequently does this role provide a briefing? At least:	☐ Semi annually	☐ Annually
Privacy Officer:	Identify the most senior role in the company having responsibility for privacy, such as CPO (chief privacy officer) or DPO (data protection officer) or functional equivalent.	

Does this role have direct responsibility for managing privacy incident response?			☐ Yes ☐ No
To whom does this role report? Select all that apply		☐ Executive officers or committee of executive officers	
☐ Board of directors	☐ Principal owners or shareholders		
Identify any other			
How frequently does this role provide a briefing? At least:		☐ Semi annually	☐ Annually
Privacy Policy:	Does the Applicant have a written privacy policy or privacy notice reviewed by an attorney and updated at least annually?		☐ Yes ☐ No
Information Security Policy:	Does the Applicant have a written information security policy?		☐ Yes ☐ No
When was this policy last updated?			
Is it based on or aligned with any of the following standards, frameworks or best practices? Select all that apply			
☐ NIST Cybersecurity Framework or other publications	☐ ISO/IEC 27001	☐ US-CERT	
Identify any other			
Business Continuity Plan:	Does the Applicant have a written business continuity plan?		☐ Yes ☐ No
How frequently is this plan tested? At least:	☐ Quarterly	☐ Semi annually	☐ Annually
Disaster Recovery Plan:	Does the Applicant have a written disaster recovery plan?		☐ Yes ☐ No
How frequently is this plan tested? At least:	☐ Quarterly	☐ Semi annually	☐ Annually
Incident Response Plan:	Does the Applicant have a written incident response plan?		☐ Yes ☐ No
How frequently is this plan tested? At least:	☐ Quarterly	☐ Semi annually	☐ Annually

Are copies of the business continuity/disaster recovery and incident response plans stored so that they will be accessible if the Applicant's network became completely unavailable?		☐ Yes ☐ No
Document Retention & Recordkeeping:	Does the Applicant have a written document retention policy?	☐ Yes ☐ No
	Does the Applicant have a written recordkeeping policy?	☐ Yes ☐ No

Do these policies enable the Applicant to identify all Personal Information subjected to the following activities during the last 12 months? Select all that apply

☐ Collection	☐ Processing	☐ Sharing	☐ Sale	☐ Deletion

Do these policies enable the Applicant to identify the source(s) from which Personal Information was collected, sold or shared?	☐ Yes ☐ No
Do these policies enable the Applicant to identify the business purpose(s) for which Personal Information was collected, sold or shared?	☐ Yes ☐ No
Additional Comments about Governance:	

COMPLIANCE

Privacy Laws:	Is the Applicant currently compliant with, or enabled to demonstrate a defensible compliance position under, the following laws? Select all that apply			
☐ GDPR	☐ CCPA	☐ PIPEDA	☐ BIPA	☐ HIPAA/HITECH
☐ GLBA	☐ FCRA/FACTA/Red Flags Rules	☐ TCPA	☐ CAN-SPAM	☐ VPPA
Identify any other				
Information Handling:	With respect to any Personal Information collected, shared or sold, does the Applicant make the following disclosures? Select all that apply			

☐ Public notice describing collection, sharing, sale and use	☐ Public notice describing individual rights regarding Personal Information including the right to restrict sale, automated decision-making or other processing and the right to access, portability, correction and deletion	☐ Individual notice at collection describing sharing, sale and use

With respect to any Personal Information collected, shared or sold, are the following processes in place?
Select all that apply

☐ Opt in/opt out of a sale of Personal Information	☐ Request to transfer Personal Information	☐ Request to correct Personal Information
☐ Request to delete Personal Information	☐ Request to know about specific Personal Information collected, sold or shared	
☐ Request to restrict processing Personal Information	☐ Request to restrict automated decision-making using Personal Information	

Does the Applicant collect Biometric Information from the following groups of individuals? Select all that apply

☐ Not collected	☐ Employees/contractors	☐ Customers	
Identify any other			

With respect to any Biometric Information collected, are the following disclosures and processes in place?
Select all that apply

☐ Public notice disclosing collection, use, processing, sharing, sale, profit from, possession, retention, security and destruction	☐ Individual notice prior to collection including use, processing, sharing, sale, profit from, possession, retention, security and destruction
☐ Individual consent or release for collection, use, processing, sharing, sale, profit from, possession, retention and destruction, in writing and reviewed by an attorney	☐ Processes to prevent improper use, processing, sharing, sale, profit from, possession, retention and destruction

☐ Written policy regarding collection, use, processing, sharing, sale, profit from, possession, storage, retention and destruction, consistent with standards in the Applicant's industry, reviewed by an attorney, and publicly available		☐ Not collected
Where is Biometric Information stored? Select all that apply	☐ Cloud	☐ Applicant's network
Is Biometric Information subject to the following measures? Select all that apply		☐ Encryption in transit

☐ Encryption at rest	☐ Restricted access on a least privilege basis	☐ Segregated in an isolated environment

Are any of the Applicant's products or services used in the collection, use, processing, sharing, sale, profit from, possession, retention or destruction of Biometric Information?	☐ Yes ☐ No

Please describe		
Does the Applicant transmit Personal Information cross border to another jurisdiction?		☐ Yes ☐ No
Is the Applicant compliant with all laws pertaining to transmission of Personal Information cross border to another jurisdiction?		☐ Yes ☐ No
PCI DSS:	Is the Applicant required to be compliant with the PCI DSS?	☐ Yes ☐ No
PCI Merchant Level (1-4):		
How many payment card transactions does the Applicant process annually?		
Is the Applicant currently compliant with the PCI DSS requirements for its merchant level?		☐ Yes ☐ No
Which version of PCI-DSS was the Applicant assessed against?		
Additional Comments about Compliance:		

CONTROLS

Maintenance:	How frequently does the Applicant update software, patch vulnerabilities, disable unnecessary services and remove unnecessary software and hardware? At least:			☐ Continuously
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Please give an overview of the Applicant's vulnerability management and critical patching process and timeline, if outside of the below:				

Critical patching target:	☐ < 24 Hours	☐ 24-72 Hours	☐ 3-7 days	☐ > 7 Days

Normal Vulnerability Management patching target:	☐ < 7 Days	☐ 7-14 Days	☐ 14-30 Days	☐ > 30 Days
How quickly are critical updates implemented following release? At least within:				
☐ 24 hours	☐ 72 hours	☐ 1 week	☐ 2 weeks	☐ 1 month
Life Cycle & Inventory Management:	Does the Applicant use any operating system, hardware or software that is no longer supported or is considered End-of-Life by the manufacturer?			☐ Yes ☐ No
If yes, please give an overview of usage, remediation plans, decommission strategy, segregation and any other additional controls or securities in place				
What percentage of hardware connected to the network is inventoried?				%
How frequently is the hardware inventory updated? At least:				☐ Continuously
☐ Quarterly	☐ Semi annually	☐ Annually		
What percentage of software connected to the network is inventoried?				%
Log Monitoring:	Please describe the Applicant's audit logging policies, anomaly review practices and log analysis solutions, such as SIEM.			
Are these policies, practices and solutions applied to the following? Select all that apply			☐ Firewalls	☐ Intrusion detection and prevention
Is the local logging performed on a per-host basis?				☐ Yes ☐ No
Are local logs centralized into a log management system?				☐ Yes ☐ No
How frequently are logs audited? At least:				☐ Continuously
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
How long are audit logs maintained? At least:		☐ 30 days	☐ 90 days	☐ 1 year

Security Configuration:	Does the Applicant employ strict security configuration management of personal devices, web applications, servers, databases and critical business and security applications?			☐ Yes ☐ No
How frequently are these security configurations updated? At least:				☐ Continuously
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Please describe any systems hardening techniques performed by the Applicant.				
Is software installation automatically controlled and unauthorized software blocked?				☐ Yes ☐ No
Testing & Scanning:	Does the Applicant conduct regular penetration testing?			☐ Yes ☐ No
How frequently is this testing conducted? At least:				
☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually	☐ Biannually
Is this testing conducted in-house or outsourced?				☐ Yes ☐ No
Does the Applicant conduct regular vulnerability scans?				☐ Yes ☐ No
How frequently is this scanning conducted? At least:				☐ Continuously
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Backups:	Does the Applicant conduct regular back up of data?			☐ Yes ☐ No
How frequently is Critical Information backed up? At least:			☐ Continuously	☐ Daily
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Which of the following does the Applicant utilize for backups?			Tapes	☐ Yes ☐ No
Disks	☐ Yes ☐ No	Cloud	☐ Yes ☐ No	
Where are backups stored? Select all that apply			MSSP	☐ Yes ☐ No
On premises	☐ Yes ☐ No	Offline storage	☐ Yes ☐ No	
Offsite storage	☐ Yes ☐ No	Secondary data center	☐ Yes ☐ No	

Please give an overview of the Applicant's backup strategy and who has access to the backup environment					
Are backups subject to the following measures?					
Multi Factor Authentication	☐ Yes ☐ No	Encryption	☐ Yes ☐ No		
Segmentation	☐ Yes ☐ No	Virus/malware scanning	☐ Yes ☐ No		
Immutable	☐ Yes ☐ No	Privileged Access Management	☐ Yes ☐ No		
Identify any additional controls/securities					
Unique backup credentials stored separately from other user credentials					☐ Yes ☐ No
If backups are encrypted, are encryption keys stored offline?					☐ Yes ☐ No
How frequently are backups made to offsite storage? At least:	☐ Daily	☐ Weekly	☐ Monthly	☐ Quarterly	
How frequently are backups made to offline storage? At least:	☐ Daily	☐ Weekly	☐ Monthly	☐ Quarterly	
How frequently is a full recovery from a backup tested? At least:		☐ Monthly	☐ Quarterly	☐ Annually	
Redundancy:	Does the Applicant employ redundancy of critical business systems?			☐ Yes ☐ No	
Intrusion Detection & Prevention:	Does the Applicant employ any intrusion detection and prevention solution?			☐ Yes ☐ No	
How frequently are intrusion logs reviewed? At least:				☐ Continuously	
☐ Daily	☐ Weekly	☐ Biweekly	☐ Monthly	☐ Quarterly	
What is the expected time to respond to an intrusion?			Hours		Minutes

Endpoint Detection & Response:	Does the Applicant employ an endpoint detection and response solution (EDR)?	☐ Yes ☐ No
If yes, what % of the Applicant's endpoints is EDR deployed on?	%	
If yes, what % of the Applicant's servers is EDR deployed on?	%	
Please identify EDR solution(s) in place, including company names & product name:		
Data Loss Prevention:	Does the Applicant employ a data loss prevention solution? Please describe	

Does the Applicant control the transmission of Personal Information, Corporate Information and Critical Information off network? Select all that apply	☐ Off network	☐ Removable media
Are removable storage devices monitored and regulated?		☐ Yes ☐ No

Mitigation Software:	Are any of the following implemented? Select all that apply	
☐ DDoS mitigation	☐ Crimeware detection software	☐ Anti-virus/anti malware software
Encryption:	Does the Applicant employ mandatory encryption to protect the following? Select all that apply	
☐ Personal Information in transit	☐ Personal Information at rest	
☐ Corporate Information in transit	☐ Corporate Information at rest	
☐ Critical Information	☐ Personal devices	☐ Removable media

Filtration:	Does the Applicant employ any of the following solutions?	SPF	☐ Yes ☐ No
DKIM	☐ Yes ☐ No	DMARC	☐ Yes ☐ No

Firewalls:	Does the Applicant employ the following firewalls? Select all that apply	☐ External or perimeter	☐ Internal
Is each firewall password protected?			☐ Yes ☐ No
IP filtering is used to prevent connections from known-malicious addresses			☐ Yes ☐ No
Network ports can only be opened with a legitimate business need			☐ Yes ☐ No
Port accessibility is regularly verified automatically			☐ Yes ☐ No
Identify all roles having access to configuring firewalls or controlling traffic across firewalls?			
How frequently is firewall configuration reviewed? At least:		☐ Semi annually	☐ Annually
How frequently is the firewall firmware updated? At least:		☐ Semi annually	☐ Annually
What is the firewall policy? Select all that apply		☐ Deny all by default, permit by exception	☐ Deny by exception

Segregation:	Has the Applicant applied network segmentation within its environment?			☐ Yes ☐ No
If yes, please indicate on what basis:	Geography	☐ Yes ☐ No	System Criticality	☐ Yes ☐ No
	Subsidiaries	☐ Yes ☐ No	Brick and Mortar Locations	☐ Yes ☐ No
	Business Function	☐ Yes ☐ No	Data Classification	☐ Yes ☐ No
Any other Network Segmentation details/points to clarify:				

Are the following segregated in an isolated environment? Select all that apply				
☐ Personal Information	☐ Corporate Information	☐ Critical servers	☐ Critical Information	
Are development, testing and production conducted in separate environments?				☐ Yes ☐ No
Access:	Is access to the network restricted on a least privilege basis?			☐ Yes ☐ No
Is access to Personal Information, Corporate Information and Critical Information restricted on a least privilege basis?				☐ Yes ☐ No

Is access audited and updated? At least:				☐ Continuously
☐ Daily	☐ Weekly	☐ Biweekly	☐ Monthly	☐ Quarterly
Is exercise of administrator and privileged access audited and updated? At least:				☐ Continuously
☐ Daily	☐ Weekly	☐ Biweekly	☐ Monthly	☐ Quarterly
Are changes to administrator accounts reported automatically?				☐ Yes ☐ No
Are all accounts associated with legitimate processes or current users?				☐ Yes ☐ No
Does the Applicant activity monitor all privileged and administrator access for unusual behavior patterns?				☐ Yes ☐ No
Does the Applicant impose minimum security requirements on all devices connecting to the network?				☐ Yes ☐ No
Is the Applicant enabled to remotely wipe personal devices that are components of its network?				☐ Yes ☐ No
Please describe any password strength, expiration and reuse policies employed by the Applicant:				
Is Multi Factor Authentication required for the following access?			Critical Information	☐ Yes ☐ No
Remote access	☐ Yes ☐ No	Third Party/Vendor Access		☐ Yes ☐ No
Personal devices	☐ Yes ☐ No	Noncritical information and applications		☐ Yes ☐ No

Does the Applicant utilize a Privileged Access Management (PAM) tool?	☐ Yes ☐ No
If yes, is access to the PAM tool subject to Multi Factor Authentication?	☐ Yes ☐ No
If no, please describe how the Applicant is securing privileged and administrator accounts:	
What secondary factor method is the Applicant using for Multi Factor Authentication?	SMS ☐ Yes ☐ No
	Non-Corporate Device (if Yes above) ☐ Yes ☐ No

Biometric Authentication ☐ Yes ☐ No	Authenticator Application ☐ Yes ☐ No	Secondary Email ☐ Yes ☐ No	Endpoint Certificate ☐ Yes ☐ No	Physical Security Keys ☐ Yes ☐ No

Identify any other:	

Please identify the number of domain and service accounts the Applicant has in the Domain Admin Group:		
Are these stored in either of the following?	Local Directory ☐ Yes ☐ No	Active Directory ☐ Yes ☐ No
Identify any other:		

Does the use and distribution of administrator and privileged access require senior management approval?	☐ Yes ☐ No
Please describe the Applicant's wireless security policies:	
Are connections from untrusted wireless devices allowed?	☐ Yes ☐ No
Do untrusted wireless devices use a separate network?	☐ Yes ☐ No

Training & Awareness:	Does the Applicant conduct mandatory information security and privacy training of employees and contractors having the following content at least annually?		
Social engineering	☐ Yes ☐ No	Phishing campaigns	☐ Yes ☐ No
Role based training	☐ Yes ☐ No	Privacy/data handling compliance	☐ Yes ☐ No
Security/threat awareness		☐ Yes ☐ No	
Identify any other			

Are Phishing Simulations conducted for all employees?					☐ Yes ☐ No
How frequently is the Applicant conducting Phishing Simulations?		☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Are Phishing Simulations:	Role Based ☐ Yes ☐ No	Targeted ☐ Yes ☐ No	Sent in a staggered fashion ☐ Yes ☐ No		
Click Rate of most recent simulation	☐ < 5%	☐ 5-10%	☐ 10-15%	☐ 15-20%	☐ > 20%

Reporting Rate of most recent simulation:	☐ < 5%	☐ 5-10%	☐ 10-15%	☐ 15-20%	☐ > 20%
Does the Applicant have a report phishing email add-in enabled for all email users?				☐ Yes ☐ No	
Does the Applicant employ a sandboxing solution for investigating suspicious emails/attachments?				☐ Yes ☐ No	
How does the Applicant handle repeat offenders/clickers?					

Does the Applicant update its information security and privacy training content and communications at least annually?			☐ Yes ☐ No
Does the Applicant require service providers and third parties having access to the Applicant's network and data to undertake information security and privacy training at least annually?			☐ Yes ☐ No
Screening:	Are job Applicants subject to screening including credit history, criminal records, drug testing as permitted by law?		☐ Yes ☐ No
Peer Sharing Groups:	Does the Applicant participate in any information security threat, vulnerability and incident sharing program to improve awareness, assessment, monitoring and response?		☐ Yes ☐ No
Physical Theft & Loss:	Does the Applicant detect when critical hardware are removed from the network?		☐ Yes ☐ No
Does the Applicant employ a procedure for reporting and recording lost or stolen hardware?			☐ Yes ☐ No
Security Management:	Are any of the following implemented? Select all that apply		
☐ Unified threat management or threat prevention systems	☐ Independent security audit or assessment		☐ Managed security services
Does the Applicant have a Security Operations Center (SOC)?			☐ Yes ☐ No
If yes:	Is it monitored 24/7?		☐ Yes ☐ No
	Is it managed internally or by a third party?	Internally	☐ Yes ☐ No
	Third party ☐ Yes ☐ No	Hybrid	☐ Yes ☐ No
Provide any other information on the Applicant's SOC			
Does the Applicant employ Microsoft (Office) 365?			☐ Yes ☐ No

If yes, are the following implemented?				
Microsoft 365 Advanced Threat Protection (ATP)/Defender	☐ Yes ☐ No	Multi Factor Authentication for all Microsoft 365 users		☐ Yes ☐ No
Is Remote Desktop Protocol (RDP) enabled?			☐ Yes ☐ No	
If yes, is RDP accessible:	Internally	☐ Yes ☐ No	Externally	☐ Yes ☐ No
If yes, are the following implemented?				
VPN access with Multi Factor Authentication only	☐ Yes ☐ No	Multi Factor Authentication for access		☐ Yes ☐ No
Network level authentication enabled		☐ Yes ☐ No	Accessible through PAM	☐ Yes ☐ No
Identify any other controls/securities in place for RDP usage:				
Additional Comments about Controls:				

BUSINESS CONTINUITY

Recovery Time:	In the event of an interruption of the Applicant's network, what is the Applicant's recovery time objective for critical systems, applications and processes? At most:			
☐ < 8 hours	☐ 8-12 hours	☐ 12-24 hours	☐ 24-48 hours	☐ > 48 hours
Have these been validated in the last 12 months?				☐ Yes ☐ No
Impact:	In the event Critical Information, or critical systems, applications or processes became unavailable, how long would it take to materially interrupt the Applicant's business? At most:			
☐ < 1 hour	☐ 1-8 hours	☐ 8-12 hours	☐ 12-24 hours	☐ 24-48 hours

Is the Applicant enabled to employ a manual workaround in the event of an interruption of the network?		☐ Yes ☐ No
Please describe		
Is the Applicant enabled to immediately failover into a redundant information system in the event of an interruption of the network?		☐ Yes ☐ No
Please describe		
Does the Applicant maintain a hot, warm or cold site backup IT facility?		☐ Yes ☐ No
Please describe		
Prior Event:	Has the Applicant experienced a partial or total network interruption lasting more than 8 hours?	☐ Yes ☐ No

SERVICE PROVIDERS

IT and Cloud-Based Services:	Identify all IT and cloud-based services providing critical business applications, infrastructure or processes. Select all that apply			
☐ Adobe	☐ AWS	☐ Dropbox	☐ Google	☐ IBM
☐ Microsoft 365	☐ Microsoft Azure	☐ Oracle	☐ Rackspace	☐ Salesforce
☐ SAP	☐ Workday	☐ Xero	☐ Zoho	

Identify any other	
Non IT Services:	Identify the five non IT service providers providing the most critical business processes to the Applicant's business.

1	2
3	4
5	

Does the Applicant review the information security and privacy controls of each of its IT, cloud-based and non IT service providers?				☐ Yes ☐ No
Does the Applicant audit the information security and privacy controls of each of its IT, cloud-based and non IT service providers?				☐ Yes ☐ No
How frequently are the audits performed?			☐ Semi annually	☐ Annually
Is service provider access to the Applicant's network or data restricted on a least privilege basis?				☐ Yes ☐ No
Please describe any other restrictions on service provider access to the network or data:				
Is service provider access to the Applicant's data or network reviewed?				☐ Yes ☐ No
How frequently are the reviews performed? At least:				☐ Continuously
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Contracts:	Does the Applicant have written agreements with all third parties having access to the Applicant's network or data?			☐ Yes ☐ No
Do all the written agreements require the third party to defend or indemnify the Applicant against liability because of a security or privacy incident on the third party's network or caused by the third party?				☐ Yes ☐ No

Do all the written agreements require the third party to procure insurance applicable to the Applicant in the event of a security or privacy incident on the third party's network or caused by the third party?	☐ Yes ☐ No
Do any of the written agreements limit the third party's liability in the event of a security or privacy incident on the third party's network?	☐ Yes ☐ No
Additional Comments about Service Providers:	

CRIME

Transactions:	What is the daily average number of transactions transferring first party funds?	
What is the average value transferred each day?		
What is the average value of any one transfer?		
Authentication & Next Level Approval:	Does the Applicant employ a protocol to confirm transfer instructions including a call back, email or an alternative method of authenticating the instruction?	☐ Yes ☐ No
Please describe		
Does the Applicant employ a protocol requiring more than one or next-level approval?		☐ Yes ☐ No
Please describe		
Anti Fraud Training	Does the Applicant conduct anti-fraud training of employees at least annually?	☐ Yes ☐ No

Prior Events:	During the last 3 years, has the Applicant experienced any fraudulent transfer or transfer instruction, social engineering, business email compromise or phishing attack?	☐ Yes ☐ No
Additional Comments about Crime:		

MEDIA

Media Activities:	Please describe the Applicant's media activities including advertising activities			
Current fiscal year budget allocation to advertising activities:				
Website Content:	What type of content does the Applicant publish or post on its website? Select all that apply			☐ No website
☐ Content created by the Applicant	☐ Licensed third party content	☐ Unlicensed third party content (message boards, reviews)		☐ Streaming video or music content
Legal Review and Clearance:	Is the content reviewed by an attorney prior to publishing or posting on any website owned or operated by the Applicant or its social media pages or under its accounts on third party websites?			☐ Yes ☐ No
Does the attorney's review screen for the following liability risks? Select all that apply				
☐ Defamation or disparagement	☐ Outrage or infliction of emotional distress	☐ Infringement of privacy or publicity rights	☐ Infringement of copyright, plagiarism or misappropriation of ideas	
Does the Applicant have a process for handling allegations that content created, displayed or published by the Applicant that is defamatory or disparaging or infringes third party copyright or privacy rights?				☐ Yes ☐ No
Does the Applicant have a written policy for handling requests for retractions or corrections?				☐ Yes ☐ No
Does the Applicant have a written policy for checking the accuracy and originality of content created by or on behalf of the Applicant?				☐ Yes ☐ No

Contracts:	Does the Applicant have written agreements with all third parties providing advertising services or providing content to or on behalf of the Applicant?	☐ Yes ☐ No
Do all the written agreements require the third party to defend or indemnify the Applicant against liability arising out of the third party's services or content?		☐ Yes ☐ No
Do all the written agreements require the third party to procure insurance applicable to the Applicant in the event of liability arising out of the third party's services or content?		☐ Yes ☐ No
Do any of the written agreements limit the third party's liability arising out of the third party's services or content?		☐ Yes ☐ No
Additional Comments about Media:		

SECURITY AND PRIVACY CLAIMS AND EVENTS

Unauthorized Disclosure:	During the last 3 years, has the Applicant experienced any failure to protect Personal Information or Corporate Information in the Applicant's or its Service Provider's care/custody/control, or for which the Applicant is legally responsible? (damage to, destruction, loss, theft, unauthorized disclosure)	☐ Yes ☐ No
Please describe		
Wrongful Collection, Retention, Use or Processing:	During the last 3 years, has the Applicant received notice of any claim, complaint or demand alleging infringement of a privacy right or failure to comply with a privacy regulation pertaining to Personal Information in the Applicant's or its Service Provider's care/custody/control, or for which the Applicant is legally responsible? (wrongful collection, retention, sale, disposal, deletion, disclosure, use, control, processing, access or correction)	☐ Yes ☐ No

Please describe		
Unauthorized Access:	During the last 3 years, has the Applicant experienced any failure of the security of its network? (intrusion, tampering, denial of service attack, insertion of virus, malware, ransomware or other malicious code, extortion demand or other unauthorized access or use)	☐ Yes ☐ No
During the last 3 years, has the Applicant received notice of any claim, complaint or demand alleging or arising out of any failure of the security of its network?		☐ Yes ☐ No
Please describe		
Prior Regulatory Actions:	During the last 3 years, has the Applicant been the subject of any civil or administrative proceeding, civil investigation or subpoena or request for information by a government agency or data protection or other organization having authority to enforce a privacy regulation authority?	☐ Yes ☐ No
Please describe		
Prior Knowledge:	Does any director, officer or employee of the Applicant, its parent company or any of its subsidiaries or affiliates have knowledge or information about any fact, circumstances, incident, event or transaction that may give rise to a claim, complaint or demand alleging a privacy or security incident or media liability?	☐ Yes ☐ No
Please describe		
Prior Notice:	Have any of these matters been reported to another insurer?	☐ Yes ☐ No

Remediation:	In response to any of these matters, has the Applicant commenced or completed any change to its network and information security and handling practices, or other changes, to remediate the effects of the matter or remove a vulnerability that gave rise to the matter?	☐ Yes ☐ No
Please describe		

REPRESENTATIONS AND SIGNATURE

By signing this document, the undersigned authorized representative of the Applicant represents on behalf of all persons and entities proposed for coverage, after inquiry, that to the best of their knowledge:

1. The statements and answers given in and all materials submitted with this Application are true, accurate and complete.
2. No facts or information material to the risk proposed for insurance have been misstated or concealed.
3. These representations are a material inducement to the Insurer to provide a proposal for insurance.
4. Any policy the Insurer issues will be issued in reliance upon these representations.
5. The Applicant will report to the Insurer immediately in writing any material change in the Applicant's activities, products and services.
6. The Applicant will report to the Insurer immediately in writing any material changes to the answers provided in this Application which occur or are discovered between the date of this Application and the effective date of the policy for which coverage is sought by submission this Application.
7. The Insurer reserves the right, upon receipt of any such notice, to modify or withdraw any proposal for insurance the Insurer has offered.

WARNING

PLEASE REVIEW THE STATE FRAUD STATEMENT CONTAINED AT THE END OF THIS APPLICATION APPLICABLE TO THE STATE IN WHICH THE APPLICANT RESIDES.

Any person who, with intent to defraud or knowingly facilitates a fraud against the insurer, submits an application or files a claim containing a false or deceptive statement may be guilty of insurance fraud.

This Application must be signed by the Applicant's Chief Executive Officer, President, Chief Information Officer, Chief Technology Officer, Chief Security Officer, Chief Operating Officer, Chief Financial Officer or General Counsel or Risk Manager, or their functional equivalent, unless the Insurer instructs the Applicant otherwise.

Name _____ Name (Signature) _____

Title _____

Date _____

TO BE COMPLETED BY PRODUCERS ONLY:

RETAIL PRODUCER		WHOLESALE PRODUCER	
Producer Name:		**Producer Name:**	
City, State:		**City, State:**	
Telephone No.:		**Telephone No.:**	
License No.:		**License No.:**	

Producer Signature: _____

STATE FRAUD STATEMENT

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 application for insurance is guilty of a crime and may be subject to restitution fines or confinement in prison or any combination thereof.

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 application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

CALIFORNIA

For your protection, California law requires the following warning 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 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 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.

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.

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.

KANSAS

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, 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.

KENTUCKY

Any person who knowingly and with intent to defraud any insurance company or other 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 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 application for insurance 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 for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

MARYLAND

Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who 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.

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 application for insurance is guilty of a crime and may be subject to civil fines and criminal penalties.

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.

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.

OKLAHOMA

WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

OREGON

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents materially false information in an application for insurance may be guilty of a crime and may be subject to fines and confinement in prison.

In order for us to deny a claim on the basis of misstatements, misrepresentations, omissions or concealments on your part, we must show that:

A. The misinformation is material to the content of the policy;

B. We relied upon the misinformation; and

C. The information was either:

1. Material to the risk assumed by us; or

2. Provided fraudulently.

For remedies other than the denial of a claim, misstatements, misrepresentations, omissions or concealments on your part must either be fraudulent or material to our interests.

With regard to fire insurance, in order to trigger the right to remedy, material misrepresentations must be willful or intentional. Misstatements, misrepresentations, omissions or concealments on your part are not fraudulent unless they are made with the intent to knowingly defraud.

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.

PUERTO RICO

Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances be present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

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 application for insurance 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 for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

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.

VIRGINIA

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.

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.

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 application for insurance is guilty of a crime and may be subject to fines and confinement in prison.