



AXIS CYBER TECHNOLOGY & MPL APPLICATION

AXIS INSURANCE

10000 Avalon Blvd. Ste. 200

Alpharetta, GA 30009

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.

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

CONTENTS

Section	Title	Pg.
1	Applicant Information	2
2	Assets	3
3	Governance	4
4	Compliance	6
5	Controls	7
6	BCP & IR	14
7	Service Providers	15

Section	Title	Pg
8	Crime	16
9	Media	17
10	Tech E&O	18
11	MPL	21
12	Claims and Events	22
13	Other Insurance	24
14	Representations and Signature	24
15	State Fraud Statement	26



1. APPLICANT INFORMATION

Organization Name:			Website(s):		
Mailing Address:					
Risk Manager Contact:	Name:		Email Address:		
Incident Response Contact:	Name:		Email Address:		
Business Activities:	Please describe the Applicant's business activities, services, and products:				
Annual Gross Revenue (Total):	Current fiscal year:		Previous fiscal year:		
Operating Cost:	Annual operating cost for current fiscal year:				
Current fiscal year budget allocation to:		IT:		Cyber security:	
Headcount:	Employees:				
Regions:	Percentage of revenue for regions where Applicant operates:	% US:		% Europe:	
		% Canada:		% AUS/NZ:	
		% UK:		% LATAM:	
				% MEA:	
				% APAC:	
				% Russia:	
For how many years has the Applicant been in business?				<input type="checkbox"/> > 5 years <input type="checkbox"/> 3-5 years	
				<input type="checkbox"/> 1-3 years <input type="checkbox"/> < 1 year	
Ownership Structure:	Category best describing ownership structure: (Select all that apply)		<input type="checkbox"/> Private <input type="checkbox"/> Publicly traded <input type="checkbox"/> Subsidiary <input type="checkbox"/> Non-profit <input type="checkbox"/> Government		
Ownership & Organization:	Has the Applicant undergone a name change or merger, acquisition or consolidation with a third party or divestiture, during the last 5 years, or does the Applicant plan to undergo a name change or merger, acquisition or consolidation with a third party or divestiture during the next 12 months?			<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Please describe:				



2. ASSETS

2.1 Personal Information:	For purposes of this application, Personal Information refers to Personally Identifiable Information, Personal Health Information, Payment Card Industry 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 records	Information from which an individual can be uniquely and reliably identified (name email address, social security number, etc.).	
PHI records	Individual's health or medical information.	
PCI records	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, or similar.	
Does the Applicant sell or share Personal Information?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant store or process Personal Information on behalf of a third party?		<input type="checkbox"/> Yes <input type="checkbox"/> No
2.2 Corporate Information:	Corporate Information refers to third party IP, trade secrets, nonpublic business information, or information that is marked "confidential".	
Does the Applicant store or process Corporate Information?		<input type="checkbox"/> Yes <input type="checkbox"/> No
2.3 Critical Information:	Critical Information refers to information systems, software, programs, applications, that are critical to the Applicant's business. These are the Applicant's "Crown Jewels" of data.	
Please describe any information considered to be Critical Information:		
Please describe any extra security measures applied to Critical Information if not covered in other questions:		
2.4 Network:		
Does the Applicant's network include the following that store or process: PII, Corp. or Critical information or support critical business process? (Select all that apply)	<input type="checkbox"/> Web applications <input type="checkbox"/> Hosted applications <input type="checkbox"/> Removable media (USBs, offline storage) <input type="checkbox"/> POS systems <input type="checkbox"/> Vehicular onboard systems <input type="checkbox"/> BYOD devices	<input type="checkbox"/> Terminals (ATMs) <input type="checkbox"/> Healthcare devices <input type="checkbox"/> Personal devices <input type="checkbox"/> Critical IoT (Security, fire, BAS) <input type="checkbox"/> AI/robotic devices <input type="checkbox"/> OT/ICS/SCADA



AXIS CYBER TECHNOLOGY & MPL APPLICATION

How many servers are on the Applicant's network?	On/Prem/Data Center:		Cloud:
Where are the servers located? (Select all that apply)	<input type="checkbox"/> US <input type="checkbox"/> Canada <input type="checkbox"/> UK	<input type="checkbox"/> Europe <input type="checkbox"/> LATAM <input type="checkbox"/> MEA	<input type="checkbox"/> AUS/NZ <input type="checkbox"/> APAC <input type="checkbox"/> Russia
2.5 Hardware Total Insurable Value:	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?		
2.6 Website:	How is the Applicant's website managed?	<input type="checkbox"/> In-house <input type="checkbox"/> Outsourced	
Do contractors or service providers have administrator privileges on the website?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:			

3. GOVERNANCE

3.1 Information Security:			
Identify the most senior role with responsibility for information security, such as CISO or equivalent:			
Does this role have direct responsibility for managing security incident response?	<input type="checkbox"/> Yes <input type="checkbox"/> No		
To whom does this role report? (Select all that apply)	<input type="checkbox"/> Executive committee or officers <input type="checkbox"/> Principal owners or shareholders <input type="checkbox"/> Board of directors	<input type="checkbox"/> CIO/CTO <input type="checkbox"/> CFO <input type="checkbox"/> CEO	<input type="checkbox"/> Other:
How frequently is a formal reporting provided?	<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi-annually <input type="checkbox"/> Annually	<input type="checkbox"/> Ad Hoc <input type="checkbox"/> Other:
Does the Applicant have a written information security policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Last updated:	
Identify any standards or frameworks the security program is based on: (Select all that apply)	<input type="checkbox"/> NIST CSF, 800-53, 171 or others <input type="checkbox"/> ISO/IEC 27001 <input type="checkbox"/> PCI-DSS	<input type="checkbox"/> CIS 18 <input type="checkbox"/> Other:	
Peer Sharing Groups: Does the Applicant participate in any information security threat, vulnerability and incident sharing program to improve awareness, assessment, monitoring and response?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Security Management: Are any of the following implemented? (Select all that apply)		<input type="checkbox"/> Independent security audit/assessment <input type="checkbox"/> Managed security services <input type="checkbox"/> Unified threat mgt./prevention systems	
Screening: Are Applicants screened, including credit history, criminal, drug testing as permitted by law?			<input type="checkbox"/> Yes <input type="checkbox"/> No
The Applicant maintains the following documents:			



AXIS CYBER TECHNOLOGY & MPL APPLICATION

<input type="checkbox"/> Business Continuity Plan	Reviewed and tested	<input type="checkbox"/> Semi-annually	<input type="checkbox"/> Annually	<input type="checkbox"/> Other:
<input type="checkbox"/> Disaster Recovery Plan	Reviewed and tested	<input type="checkbox"/> Semi-annually	<input type="checkbox"/> Annually	<input type="checkbox"/> Other:
<input type="checkbox"/> Incident Response Plan	Reviewed and tested	<input type="checkbox"/> Semi-annually	<input type="checkbox"/> Annually	<input type="checkbox"/> Other:
Are copies of the above stored and accessible even if the network is unavailable?				<input type="checkbox"/> Yes <input type="checkbox"/> No
Identify IR playbooks in place and tested:	<input type="checkbox"/> None <input type="checkbox"/> Ransomware <input type="checkbox"/> Business Email Compromise <input type="checkbox"/> Other:			
Additional Comments:				
3.2 Privacy:				
Identify the most senior role with privacy responsibility, such as CPO, DPO, or equivalent:				
Does this role have direct responsibility for managing privacy incident response?				<input type="checkbox"/> Yes <input type="checkbox"/> No
To whom does this role report? (Select all that apply)		<input type="checkbox"/> Executive committee or officers <input type="checkbox"/> Principal owners or shareholders	<input type="checkbox"/> Board of directors <input type="checkbox"/> Other:	
How frequently is a formal reporting provided?	<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi-annually <input type="checkbox"/> Annually	<input type="checkbox"/> Ad Hoc <input type="checkbox"/> Other:	
Does the Applicant have a written privacy policy or notice?		<input type="checkbox"/> Yes <input type="checkbox"/> No	Last reviewed by attorney:	
Does the organization have user preference/behavior tracking functionality on their website?				<input type="checkbox"/> Yes <input type="checkbox"/> No
This data is:		<input type="checkbox"/> Provided to a 3 rd party or <input type="checkbox"/> Maintained in house?		
Are contractual provisions in place that detail what data will be collected?				<input type="checkbox"/> Yes <input type="checkbox"/> No
If a 3 rd party, has a code review been performed to ensure only agreed data is transmitted?				<input type="checkbox"/> Yes <input type="checkbox"/> No
Is Meta/Facebook or Google analytics providing this service?				<input type="checkbox"/> Yes <input type="checkbox"/> No
3.3 Document Retention & Recordkeeping:		Does the Applicant have a written document retention policy?		<input type="checkbox"/> Yes <input type="checkbox"/> No
		Does the Applicant have a written recordkeeping policy?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Do these policies enable the Applicant to identify all Personal Information (PI) subjected to the following activities during the last 12 months? (Select all that apply)			<input type="checkbox"/> Collection <input type="checkbox"/> Processing <input type="checkbox"/> Sharing	<input type="checkbox"/> Sale <input type="checkbox"/> Deletion
Can the Applicant identify the source(s) where PI is collected, sold, or shared?				<input type="checkbox"/> Yes <input type="checkbox"/> No
Can the Applicant identify the business purpose(s) for which PI was collected, sold, or shared?				<input type="checkbox"/> Yes <input type="checkbox"/> No



Additional Comments:

4. COMPLIANCE

4.1 Privacy Laws:			
Is the Applicant currently compliant with, or enabled to demonstrate a defensible compliance position under, the following laws?	<input type="checkbox"/> GDPR <input type="checkbox"/> GLBA <input type="checkbox"/> CCPA <input type="checkbox"/> PIPEDA	<input type="checkbox"/> TCPA <input type="checkbox"/> BIPA <input type="checkbox"/> VPPA <input type="checkbox"/> CAN-SPAM	<input type="checkbox"/> FCRA/FACTA/Red Flags Rules <input type="checkbox"/> Other:

Additional Comments:

4.2 Information Handling:	
Identify disclosures made with respect to PI:	
<input type="checkbox"/> Public notice describing individual rights regarding Personal Information (PI) including the right to restrict sale, automated decision-making or other processing and the right to access, portability, correction, and deletion. <input type="checkbox"/> Public notice describing collection, sharing, sale and use. <input type="checkbox"/> Individual notice at collection describing sharing, sale, and use.	
Identify the processes in place for PI collected, shared, or sold: (Select all that apply)	
<input type="checkbox"/> Opt in/out of a sale of PI <input type="checkbox"/> Request to transfer PI <input type="checkbox"/> Request to correct PI <input type="checkbox"/> Request to delete PI	<input type="checkbox"/> Request to know about specific PI collected, sold, or shared <input type="checkbox"/> Request to restrict automated decision-making using PI <input type="checkbox"/> Request to restrict processing PI

Does the Applicant collect Biometric Information (BI)?	<input type="checkbox"/> Employees/contractors <input type="checkbox"/> Customers	<input type="checkbox"/> Not collected <input type="checkbox"/> Other:
--	--	---

With respect to any Biometric Information (BI) collected, are the following disclosures and processes in place?

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

Where is BI stored? (Select all that apply)	<input type="checkbox"/> Cloud <input type="checkbox"/> Applicant's network <input type="checkbox"/> Other:
---	---

Is BI subject to the following? (Select all that apply)	<input type="checkbox"/> Encryption in transit <input type="checkbox"/> Encryption at rest	<input type="checkbox"/> Restricted access on a least privilege basis <input type="checkbox"/> 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?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Please describe:			
Does the Applicant transmit Personal Information across borders to another jurisdiction?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Is the Applicant compliant with all laws pertaining to cross border transmission of PI?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
4.3 PCI: Is the Applicant required to be PCI-DSS compliant?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Is the Applicant PCI compliant?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Est. # of annual PCI transactions?	Merchant Level:
Is a payment processor used?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Are they assessed for PCI compliance annually?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Identify additional PCI controls: <input type="checkbox"/> P2PE <input type="checkbox"/> Tokenization <input type="checkbox"/> Key storage off client network <input type="checkbox"/> PCI training to critical staff			
Is Applicant required to be HIPAA compliant?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Is Applicant HIPAA compliant?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:			

5. CONTROLS

5.1 Vulnerabilities & Patching: Does the Applicant maintain a documented vulnerability management plan?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
If "Yes", does it identify target timeframes for addressing Critical, High, Med, and Low vulnerabilities?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Is application of Zero-day and Emergency patches expedited?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If "Yes", please identify target timeframes:	
Please identify the target timeframe for addressing Critical/High vulnerabilities (CVSS 7.0-10.0):	<input type="checkbox"/> < 24 Hours	<input type="checkbox"/> 3-7 days	
	<input type="checkbox"/> 24-72 Hours	<input type="checkbox"/> > 7 days	
Please identify your standard cadence for addressing Medium or Low vulnerabilities:	<input type="checkbox"/> < 30 days	<input type="checkbox"/> 60-90 days or greater	
	<input type="checkbox"/> 30-60 days	<input type="checkbox"/> Ad Hoc only	
Does the Applicant receive threat/vulnerability alerts from external sources?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Does the Applicant use a solution to identify vulnerabilities, track remediation and/or identify trends?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If "Yes", please identify solution:	
A formal process exists for assessing vulnerabilities potential impact to Applicant's environment:			<input type="checkbox"/> Yes <input type="checkbox"/> No
Indicate frequency of internal scanning:	<input type="checkbox"/> Continuously <input type="checkbox"/> Daily	<input type="checkbox"/> Weekly <input type="checkbox"/> Monthly	<input type="checkbox"/> Quarterly <input type="checkbox"/> Twice/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:



AXIS CYBER TECHNOLOGY & MPL APPLICATION

Indicate frequency of external scanning :	<input type="checkbox"/> Continuously <input type="checkbox"/> Daily	<input type="checkbox"/> Weekly <input type="checkbox"/> Monthly	<input type="checkbox"/> Quarterly <input type="checkbox"/> Twice/yr.	<input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc	<input type="checkbox"/> Never <input type="checkbox"/> Other:
Percent of environment covered by scans:	% (If <100% please provide detail in Additional Comments below)				
Additional Comments: (Please give an overview of the Applicant's vulnerability management and critical patching process and timeline, if outside of the above):					
<hr/>					
5.2 Pen Testing:	The Applicant conducts regular penetration testing? (Select all that apply and frequency below) <input type="checkbox"/> No				
<input type="checkbox"/> External-network	<input type="checkbox"/> Quarterly <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:				
<input type="checkbox"/> Internal-network	<input type="checkbox"/> Quarterly <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:				
<input type="checkbox"/> Social engineering	<input type="checkbox"/> Quarterly <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:				
<input type="checkbox"/> Physical	<input type="checkbox"/> Quarterly <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:				
<input type="checkbox"/> Web App.	<input type="checkbox"/> Quarterly <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:				
<input type="checkbox"/> Other:	<input type="checkbox"/> Quarterly <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Never <input type="checkbox"/> Other:				
Testing is conducted:	<input type="checkbox"/> Internally <input type="checkbox"/> Outsourced				
Additional Comments:					
<hr/>					
5.3 Life Cycle & Inventory Mgt:	Does the Applicant use any operating system, hardware or software that is no longer supported or is considered End-of-Life (EoL) by the manufacturer?				<input type="checkbox"/> Yes <input type="checkbox"/> No
If "Yes", please identify the EoL component(s):			If "Yes", please identify their function:		
Please indicate the controls applied to EoL components:		<input type="checkbox"/> Known and Inventoried <input type="checkbox"/> Decomm/replacement plans in place <input type="checkbox"/> Additional service purchased	<input type="checkbox"/> Tracked and reported <input type="checkbox"/> Monitoring and alerting <input type="checkbox"/> Segmented	<input type="checkbox"/> Other:	
Are ALL EoL components covered by controls above:			<input type="checkbox"/> All covered <input type="checkbox"/> Some not covered (Please provide detail in Additional Comments below)		
An up-to-date hardware and software inventory is maintained?				<input type="checkbox"/> Yes <input type="checkbox"/> No	
Inventory processes are:		<input type="checkbox"/> Manual <input type="checkbox"/> Semi-automated <input type="checkbox"/> Fully automated			
Hardware inventory updates occur:		<input type="checkbox"/> Continuously <input type="checkbox"/> 2x/yr. <input type="checkbox"/> Other: <input type="checkbox"/> Quarterly <input type="checkbox"/> Annually		Percentage of hardware inventoried: %	



Percentage of software inventoried?	%	Are users allowed to install applications?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:			
5.4 SOC/SIEM:	Does the Applicant use a SIEM?	<input type="checkbox"/> Yes (If yes, please identify the solution): <input type="checkbox"/> No (Please provide detail in Additional Comments below)	
Is the SIEM tuned for your org. with 100% network log coverage?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If any, identify systems whose logs are excluded from SIEM:	
How frequently are logs reviewed?	<input type="checkbox"/> Continuously <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly	<input type="checkbox"/> Quarterly <input type="checkbox"/> Semi-annually <input type="checkbox"/> Annually	How long are audit logs maintained? At least: <input type="checkbox"/> 30 days <input type="checkbox"/> 90 days <input type="checkbox"/> 1 year or greater
Is a Security Operations Center (SOC) used?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If yes: <input type="checkbox"/> Staffed 24/7/365 "eyes on glass" <input type="checkbox"/> Other: <input type="checkbox"/> Internal staff <input type="checkbox"/> External staff <input type="checkbox"/> SOC staff can take responsive or corrective action in event of alert.	
If 3 rd party/MSSP, please indicate contractual notification and response time (Days/Hours/Mins):			
Additional Information: If SOC/SIEM not used, please identify alert notification and handling processes:			
5.5 Security Configuration:	Hardened configs are used for:		
	<input type="checkbox"/> Laptops <input type="checkbox"/> Workstations <input type="checkbox"/> Mobile devices <input type="checkbox"/> Web apps	<input type="checkbox"/> Servers <input type="checkbox"/> Databases <input type="checkbox"/> Security applications	<input type="checkbox"/> Not used <input type="checkbox"/> Other:
Security configurations are updated at least:	<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi-annually <input type="checkbox"/> Annually	<input type="checkbox"/> Other:
Indicate hardening standards used:	<input type="checkbox"/> Center for Internet Security <input type="checkbox"/> Microsoft <input type="checkbox"/> NIST <input type="checkbox"/> SANS <input type="checkbox"/> Other:		
Additional Comments:			
Is software installation automatically controlled and unauthorized software blocked?			<input type="checkbox"/> Yes <input type="checkbox"/> No
5.6 Backups & Redundancy:	Critical back-ups are completed:	<input type="checkbox"/> Continuously <input type="checkbox"/> Weekly <input type="checkbox"/> Other: <input type="checkbox"/> Daily <input type="checkbox"/> Monthly	
Which of the following does the Applicant utilize for backups?		<input type="checkbox"/> Tapes <input type="checkbox"/> Cloud <input type="checkbox"/> Disk <input type="checkbox"/> Other:	
Back-ups are stored:	<input type="checkbox"/> On premises <input type="checkbox"/> Offline <input type="checkbox"/> Offsite <input type="checkbox"/> Secondary Data Center <input type="checkbox"/> MSSP <input type="checkbox"/> Other:		



Indicate existing backup controls:	<input type="checkbox"/> Segmentation <input type="checkbox"/> Malware Scanning <input type="checkbox"/> Unique Backup Accounts (stored separately) <input type="checkbox"/> Encryption <input type="checkbox"/> Immutable <input type="checkbox"/> Priv. Access Mgt. <input type="checkbox"/> Other:		
If encrypted, are keys stored offline?	<input type="checkbox"/> No <input type="checkbox"/> Yes	If offline, how often is data moved?	<input type="checkbox"/> Continuously <input type="checkbox"/> Weekly <input type="checkbox"/> Quarterly <input type="checkbox"/> Daily <input type="checkbox"/> Monthly <input type="checkbox"/> Other:
Full, or large scale, restoration is tested:	<input type="checkbox"/> Quarterly <input type="checkbox"/> Twice annually <input type="checkbox"/> Annually <input type="checkbox"/> Not tested <input type="checkbox"/> Other:		
Identify redundancy or resiliency solutions in place:	<input type="checkbox"/> Hot Site <input type="checkbox"/> Warm Site <input type="checkbox"/> Snapshots <input type="checkbox"/> Failover environment <input type="checkbox"/> Other:		
Additional Comments:			
5.7 Intrusion Detection & Prevention:	Does the Applicant employ any intrusion detection and prevention solution?		<input type="checkbox"/> Yes <input type="checkbox"/> No
	How frequently are intrusion logs reviewed? At least:	<input type="checkbox"/> Continuously <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Bi-weekly <input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly	
What is the expected time to respond to an intrusion?		Hours:	Minutes:
5.8 Malware Detection & Response:	Does the Applicant employ an endpoint detection and response solution (EDR or similar) with behavioral analysis/anomaly detection?		<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, on what % of endpoints is the solution deployed?		Endpoints: %	Servers: %
Please identify the EDR (or similar) solution(s) in place (Company/product name):			
Is the solution tuned to block threats?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Is DDoS mitigation in place?	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.9 Data Loss Prevention (DLP):	Does the Applicant employ a DLP solution?		<input type="checkbox"/> Yes <input type="checkbox"/> No
	If "Yes", identify the solution(s) in place (Company/product name):		
Does the Applicant control the transmission of Personal Information, Corporate Information and Critical Information off network?	<input type="checkbox"/> Off network <input type="checkbox"/> Email <input type="checkbox"/> Removable media <input type="checkbox"/> Internet/Cloud <small>(data storage sites, message boards, etc.)</small>		
Are removable storage devices monitored and regulated?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Are data threshold alerts in place (exfiltration, deletion, movement)?			<input type="checkbox"/> Yes <input type="checkbox"/> No
5.10 Encryption:	Does the Applicant employ mandatory encryption to protect the following? (Select all that apply)		
<input type="checkbox"/> Information in transit <input type="checkbox"/> Information at rest	<input type="checkbox"/> Corporate Information at rest <input type="checkbox"/> Corporate Information in transit	<input type="checkbox"/> Critical Information <input type="checkbox"/> Removable media	<input type="checkbox"/> Personal devices <input type="checkbox"/> Other:
5.11 Email Security:	Please identify the email security controls in place:		



<input type="checkbox"/> DKIM <input type="checkbox"/> DMARC <input type="checkbox"/> SPF	<input type="checkbox"/> Quarantine <input type="checkbox"/> Block suspicious senders? <input type="checkbox"/> Block malware/phishing/SPAM?	<input type="checkbox"/> Tag/notify external email <input type="checkbox"/> Block malicious attachments/content? <input type="checkbox"/> Macros disabled	<input type="checkbox"/> Sandboxing <input type="checkbox"/> Other:	
Does the Applicant employ Microsoft (Office) 365?		<input type="checkbox"/> Yes <input type="checkbox"/> No	If yes, is MS365 ATP/Defender used? If yes, what is your MS Secure Score %?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If other cloud-based email/controls, please identify:				
Additional Comments:				
<hr/>				
5.12 Firewalls:		Does the Applicant employ the following firewalls?	<input type="checkbox"/> External or perimeter <input type="checkbox"/> Internal	
		Are default passwords changed?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
IP filtering is used to prevent connections from known-malicious addresses?				<input type="checkbox"/> Yes <input type="checkbox"/> No
Network ports can only be opened with a legitimate business need?				<input type="checkbox"/> Yes <input type="checkbox"/> No
Port restrictions, configurations, etc. are verified:		<input type="checkbox"/> Semi-annually <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Other:		
What is the firewall policy? (Select all that apply)		<input type="checkbox"/> Deny all by default, permit by exception <input type="checkbox"/> Deny by exception <input type="checkbox"/> Other:		
Additional Comments:				
<hr/>				
5.13 Segmentation:		Are the following segregated in an isolated environment?	<input type="checkbox"/> Personal Information <input type="checkbox"/> Critical servers	<input type="checkbox"/> Corporate Information <input type="checkbox"/> Critical Information
Indicate any existing network segmentation:	<input type="checkbox"/> Geographic <input type="checkbox"/> IT Management <input type="checkbox"/> Business Function <input type="checkbox"/> Subsidiaries	<input type="checkbox"/> Guest wireless <input type="checkbox"/> Servers <input type="checkbox"/> OT <input type="checkbox"/> None	<input type="checkbox"/> Other:	
How is segmentation accomplished?	<input type="checkbox"/> Firewalls <input type="checkbox"/> Sep. Domains <input type="checkbox"/> VLAN's <input type="checkbox"/> Other (Please provide detail in Additional Comments below)			
Are development, testing and production conducted in separate environments?				<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:				
<hr/>				
5.14 Access:		Is network and information access based on a least privilege basis?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Is a formal process in place for assigning access for all hires, terms, and changes?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If "Yes", is it: <input type="checkbox"/> Manual <input type="checkbox"/> Semi-automated <input type="checkbox"/> Fully automated <input type="checkbox"/> Other:		
User access is reviewed and updated:	<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Annually <input type="checkbox"/> Never <input type="checkbox"/> Other:			



Admin/privileged access is reviewed & updated:		<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Annually <input type="checkbox"/> Never <input type="checkbox"/> Other:	
Does the Applicant impose minimum security requirements on all devices connecting to the network?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant use a Mobile Device management (MDM) solution that allows remote wipe?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Passwords: Please identify any required password elements:	<input type="checkbox"/> Min. char. length 10 or > <input type="checkbox"/> Min. char. length 9 or < <input type="checkbox"/> Upper/Lower/Special char.	<input type="checkbox"/> Expiration every 6 months or less <input type="checkbox"/> Check for cracked/common passwords <input type="checkbox"/> Lockout after 6 invalid attempts	<input type="checkbox"/> Dictionary check <input type="checkbox"/> Passphrase <input type="checkbox"/> Other:
Additional Information:			
5.15 Domain/Privileged Accounts & Controls:	Please identify domain admin/priv. account controls in place?	<input type="checkbox"/> Separate accts. <input type="checkbox"/> PAM/Pwd vault <input type="checkbox"/> PAM (Check In/Out) <input type="checkbox"/> Priv. Access Workstations	<input type="checkbox"/> Other:
If PAM or Vault:	<ul style="list-style-type: none"> • Is a separate MFA instance required to access this? • Are all domain admin accounts (incl. service accounts) maintained in the solution? 		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
Total # of:	Domain Admin. Accounts:	Service Accounts w/ Domain Admin rights:	
If only admin passwords, define requirements:	Min. length:	Rotation:	Complexity:
Is all domain admin account activity logged and monitored for unusual behavior?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Are changes to admin/privileged accounts monitored and alerted automatically?			<input type="checkbox"/> Yes <input type="checkbox"/> No
All service accts have interactive login disabled?	<input type="checkbox"/> Yes <input type="checkbox"/> No (If "No", indicate # of accounts with login enabled and why in Additional Comments below)		
Indicate number of users with Local Admin rights on their systems: (Please provide detail in Additional Comments below, if needed):	<input type="checkbox"/> None <input type="checkbox"/> Limited # of users <input type="checkbox"/> Other: <input type="checkbox"/> All <input type="checkbox"/> LAPS or similar control in place <input type="checkbox"/> No controls in place		
Additional Comments:			
5.16 Access:	MFA is required for the following access: (Please provide detail in Additional Comments below, if needed)		
<input type="checkbox"/> All Admin/Privileged access (On-prem AND remote) <input type="checkbox"/> All access to cloud-based solutions <input type="checkbox"/> All remote access into network <input type="checkbox"/> Remote access by vendors/contractors	<input type="checkbox"/> Access to backups <input type="checkbox"/> Access to Remote Desktop Protocol or similar <input type="checkbox"/> Access to cloud email (i.e.:MS365) <input type="checkbox"/> Other:		



AXIS CYBER TECHNOLOGY & MPL APPLICATION

What MFA methods are in use?	<input type="checkbox"/> Secondary Email <input type="checkbox"/> SMS/Text <input type="checkbox"/> Biometrics	<input type="checkbox"/> Authenticator App <input type="checkbox"/> Physical keyfob/card <input type="checkbox"/> Other:	<input type="checkbox"/> Endpoint Cert.(Please indicate where used):
Additional Comments:			
Wireless:	Does the Applicant maintain wireless security policies:	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Are connections from untrusted wireless devices allowed?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If, yes, do untrusted wireless devices use a separate network?	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.17 Training & Awareness:	Annual training is required for:	<input type="checkbox"/> Employees/Contractors <input type="checkbox"/> Vendors <input type="checkbox"/> Ad hoc only <input type="checkbox"/> Not Required	Please indicate topics: <input type="checkbox"/> Threats <input type="checkbox"/> Privacy <input type="checkbox"/> Social Eng. <input type="checkbox"/> Regulations/Policy <input type="checkbox"/> Role-based <input type="checkbox"/> Data Handling <input type="checkbox"/> Phishing <input type="checkbox"/> Other:
Are Phishing simulations conducted for all employees?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If "Yes", indicate frequency:	<input type="checkbox"/> Monthly <input type="checkbox"/> Twice Annually <input type="checkbox"/> Ad Hoc <input type="checkbox"/> Quarterly <input type="checkbox"/> Annually <input type="checkbox"/> Other:
Are Phishing Simulations:	<input type="checkbox"/> Role Based <input type="checkbox"/> Targeted <input type="checkbox"/> Staggered		
What % of staff are covered in each simulation?	<input type="checkbox"/> 100% <input type="checkbox"/> 25% or less <input type="checkbox"/> 25 to 50% <input type="checkbox"/> 50% to 75% <input type="checkbox"/> Other:		
Click rate of most recent simulation:	<input type="checkbox"/> <5% <input type="checkbox"/> 5-10% <input type="checkbox"/> 10-15% <input type="checkbox"/> 15-20% <input type="checkbox"/> >20% <input type="checkbox"/> Other:		
What is the most recent reporting rate?	<input type="checkbox"/> <5% <input type="checkbox"/> 5-10% <input type="checkbox"/> 10-15% <input type="checkbox"/> 15-20% <input type="checkbox"/> >20% <input type="checkbox"/> Other:		
Does the Applicant require additional training on failure?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant have a report phishing email add-in enabled for all email users?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant employ a sandboxing solution for investigating suspicious emails/attachments?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Is information security and privacy training content reviewed at least annually?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Are service providers/3rd parties with access to the network required to take this training annually?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:			
5.18 RDP/SMB	Is RDP or other remote connection solution enabled?	<input type="checkbox"/> Yes <input type="checkbox"/> No	



If "Yes", is RDP or other accessible:	<input type="checkbox"/> Internally <input type="checkbox"/> Externally (public) <input type="checkbox"/> External only after remote connection/VPN		
Indicate additional controls:	<input type="checkbox"/> Restricted to IT personnel	<input type="checkbox"/> Sep. accounts required	<input type="checkbox"/> Network authentication
	<input type="checkbox"/> Alerting and monitoring for each use	<input type="checkbox"/> Accessible through PAM	<input type="checkbox"/> Other:
	<input type="checkbox"/> Lockout after failed attempts		
Is SMB v.1 or v.2 available/in use on your network?	<input type="checkbox"/> Yes <input type="checkbox"/> No		
Additional Comments:			

6. BUSINESS CONTINUITY AND INCIDENT RESPONSE

6.1 Recovery Time:			
In the event of a network interruption what is the Applicant's recovery time objective for critical systems, applications, and processes? At most:	<input type="checkbox"/> < 8 hours <input type="checkbox"/> 8-12 hours	<input type="checkbox"/> 12-24 hours <input type="checkbox"/> 24-48 hours	<input type="checkbox"/> > 48 hours <input type="checkbox"/> Other:
Have these been validated in the last 12 months?			<input type="checkbox"/> Yes <input type="checkbox"/> No
6.2 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:	<input type="checkbox"/> < 1 hour <input type="checkbox"/> 1-8 hours	<input type="checkbox"/> 8-12 hours <input type="checkbox"/> 12-24 hours	<input type="checkbox"/> 24-48 hours <input type="checkbox"/> Other:
Does the Applicant have a manual workaround in the event of an interruption of the network?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe:			
Does the Applicant have immediate failover capacity in the event of a critical network interruption?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe:			
Does the Applicant maintain a hot, warm, or cold site backup IT facility?		<input type="checkbox"/> None <input type="checkbox"/> Hot <input type="checkbox"/> Warm <input type="checkbox"/> Cold	
Please describe:			
6.3 Incident Response:			
Does the Applicant have a written Incident Response Plan (IRP) reviewed annually?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant have ransomware and/or other playbooks?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Has the Applicant completed table-top or similar testing of the IRP in last 12 months?			<input type="checkbox"/> Yes <input type="checkbox"/> No



Additional Comments:	
6.4 Prior Event:	Has the Applicant experienced a partial or total network interruption lasting more than 8 hours? <input type="checkbox"/> Yes <input type="checkbox"/> No

7. SERVICE PROVIDERS

7.1 IT and Cloud-Based Services:	Identify top 10 IT and cloud-based services providing critical business applications, infrastructure, or processes:
---	---

Service Provider Name	Service(s)	Service Provider Name	Service(s)
1.	1.	6.	6.
2.	2.	7.	7.
3.	3.	8.	8.
4.	4.	9.	9.
5.	5.	10.	10.

Identify top 10 security providers and services , such as MSSP, consulting, pen-testing, or similar:

Service Provider Name	Service(s)	Service Provider Name	Service(s)
1.	1.	6.	6.
2.	2.	7.	7.
3.	3.	8.	8.
4.	4.	9.	9.
5.	5.	10.	10.

Indicate the elements included in the Applicant's 3 rd party review process:	<input type="checkbox"/> Security Program <input type="checkbox"/> Data provided to vendor <input type="checkbox"/> Periodic Review based on risk <input type="checkbox"/> In/External Audits <input type="checkbox"/> Services and changes <input type="checkbox"/> No Review process <input type="checkbox"/> Tech. changes <input type="checkbox"/> Leadership changes
---	---

7.2 Non-IT Services:	Identify the top 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 security/privacy controls of each of its IT, cloud-based and non-IT service providers?	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Ad hoc <input type="checkbox"/> During onboarding <input type="checkbox"/> Risk-based	<input type="checkbox"/> Documented procedure <input type="checkbox"/> On contract renewal <input type="checkbox"/> Defined intervals	



Is service provider access to the Applicant's network or data restricted on a least privilege basis?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Is service provider access to the Applicant's data or network reviewed?	<input type="checkbox"/> Yes (if "Yes", indicate frequency) <input type="checkbox"/> No	<input type="checkbox"/> Continuously <input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi-annually <input type="checkbox"/> Annually <input type="checkbox"/> Other:
	Additional Comments:		
7.3 Contracts:	Does the Applicant have written agreements with all third parties having access to the Applicant's network or data?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Do all 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?		<input type="checkbox"/> Yes <input type="checkbox"/> 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?		<input type="checkbox"/> Yes <input type="checkbox"/> 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?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Additional Comments:			

8. CRIME

Respond to the questions in this section only if applying for Crime coverage

8.1 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?		
8.2 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe:		
Does the Applicant employ a protocol requiring more than one or next-level approval?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe:		



8.3 Anti-Fraud Training:	Does the Applicant conduct anti-fraud training of employees at least annually?	<input type="checkbox"/> Yes <input type="checkbox"/> No
8.4 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:		

9. MEDIA

Respond to the questions in this section only if applying for Media coverage

9.1 Media Activities:	Please describe the Applicant's media activities including advertising activities:		
Current fiscal year budget allocation to advertising activities:			
9.2 Website Content:			
What type of content does the Applicant publish or post on its website? (Select all that apply)	<input type="checkbox"/> Unlicensed third-party content (message boards, reviews) <input type="checkbox"/> Content created by the Applicant <input type="checkbox"/> Licensed third party content	<input type="checkbox"/> Streaming video or music content <input type="checkbox"/> No website	
9.3 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?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the attorney's review screen for the following liability risks? (Select all that apply)	<input type="checkbox"/> Defamation or disparagement <input type="checkbox"/> Outrage or infliction of emotional distress	<input type="checkbox"/> Infringement of copyright, plagiarism or misappropriation of ideas <input type="checkbox"/> Infringement of privacy or publicity rights	
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?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Does the Applicant have a written policy for handling requests for retractions or corrections?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Does the Applicant have a written policy for checking the accuracy and originality of content created by or on behalf of the Applicant?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
9.4 Contracts:	Does the Applicant have written agreements with all third parties providing advertising services or providing content to or on behalf of the Applicant?		<input type="checkbox"/> Yes <input type="checkbox"/> No



AXIS CYBER TECHNOLOGY & MPL APPLICATION

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?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do any of the written agreements limit the third party's liability arising out of the third party's services or content?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Additional Comments:	

10. TECH E&O

Respond to the questions in this section only if applying for Tech E&O coverage

10.1 Annual Gross Revenue (Technology Services and Products):	Annual gross revenue derived from technology services and products projected for current fiscal year:	
	Annual gross revenue derived from technology services and products projected for next fiscal year:	
	Annual gross revenue derived from technology services and products for previous fiscal year:	
10.2 Client Engagements:	Provide the following for the Applicant's 5 largest client engagements, by the revenue derived from the engagement, during the last 5 years:	
Client Name	Revenue	
1.	1.	
2.	2.	
3.	3.	
4.	4.	
5.	5.	
10.3 Technology Services and Products:	Does the Applicant provide any of the following technology services and products? Select all that apply and indicate the percentage of the Applicant's total operations involving the service or product (must equal 100%)	
Bulletin board, chat, forum or other interactive electronic environment or virtual community	<input type="checkbox"/>	%
Client relationships management (CRM) or enterprise risk management (ERM) or supply chain software	<input type="checkbox"/>	%
Computer aided design, manufacturing or drafting (CAD/CAM)	<input type="checkbox"/>	%



AXIS CYBER TECHNOLOGY & MPL APPLICATION

Data analytics or mining, processing, storage or encryption	<input type="checkbox"/>	%
E-commerce service	<input type="checkbox"/>	%
Electronic auction services	<input type="checkbox"/>	%
Hardware – manufacturing and design of hardware, components and equipment	<input type="checkbox"/>	%
Hardware – sales, installation and maintenance	<input type="checkbox"/>	%
Information Technology (IT) – technical support, maintenance, testing or training, business process outsourcing	<input type="checkbox"/>	%
Information Technology (IT) – systems analysis, design, engineering, audit, programming or implementation and related consulting	<input type="checkbox"/>	%
Internet service provider (ISP), domain name services, search engine, email or instant messaging (IM)	<input type="checkbox"/>	%
Internet media or online advertising or branding	<input type="checkbox"/>	%
Managed network or security services or hosting, cloud or colocation	<input type="checkbox"/>	%
Payment processing services	<input type="checkbox"/>	%
Sale, lease or licensing of proprietary technology or telecommunications products to others	<input type="checkbox"/>	%
Where is the proprietary technology hosted? Select all that apply	<input type="checkbox"/> Cloud hosted	<input type="checkbox"/> Client hosted
	<input type="checkbox"/> Hosted by the Applicant (ASP or SaaS)	
Sale, lease or licensing of third party technology or telecommunications products to others – nonproprietary and value added resale (VAR)	<input type="checkbox"/>	%
Software development and design – custom	<input type="checkbox"/>	%
<ul style="list-style-type: none"> Does the Applicant perform any integration of custom software into the client’s network? 	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Software development and design – packaged	<input type="checkbox"/>	%
Web page development, design and related consulting	<input type="checkbox"/>	%
Website hosting or administration or web portal services	<input type="checkbox"/>	%
Other technology services or products. Please describe:	<input type="checkbox"/>	%
10.4 Subcontractors:	Does the Applicant use subcontractors, independent contractors or other third party vendor to provide its technology services and products?	
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
What percentage of the Applicant’s technology services and products are provided by outsourcing?		
Does the Applicant have standard written agreements with the vendors for all vendor services and products?		
<input type="checkbox"/> Yes <input type="checkbox"/> No		
Do the standard agreements include any of the following? Select all that apply:		
<input type="checkbox"/> Transfer of ownership to the Applicant of all deliverables	<input type="checkbox"/> Require the vendor to defend and indemnify the Applicant against liability for harm caused by the vendor	
Are non standard agreements, or deviations from the standard agreement, reviewed by an attorney?		
<input type="checkbox"/> Yes <input type="checkbox"/> No		
10.5 Client Engagements:	Does the Applicant have standard written agreements with clients for all technology services and products?	
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Do the standard agreements include any of the following limitations of liability? Select all that apply:		



<input type="checkbox"/> Disclaimer of consequential or indirect damages	<input type="checkbox"/> Monetary cap on direct damages
<input type="checkbox"/> Disclaimer of warranties	
What percentage of the Applicant's engagements are not subject to the standard agreement?	
Are non-standard agreements, or deviations from the standard agreement, reviewed by an attorney?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.6 Project Management:	Does the Applicant have any of the following project management protocols and procedures? (Select all that apply):
<input type="checkbox"/> Scope of work, specifications, requirements and deliverables	<input type="checkbox"/> Customer acceptance signoff process
<input type="checkbox"/> Timeline and milestones and milestone review process	<input type="checkbox"/> Complaint resolution or escalation process
<input type="checkbox"/> Change order process	
10.7 Quality Controls:	Does the Applicant have any of the following quality control and customer support resources, protocols and procedures? Select all that apply:
<input type="checkbox"/> Beta testing or user acceptance testing	<input type="checkbox"/> Written product recall process
<input type="checkbox"/> Post project review process	<input type="checkbox"/> Vendor or VAR certification process
<input type="checkbox"/> Client relationship management staff	<input type="checkbox"/> Process for identifying quality control issues
10.8 Software Copyright Clearance:	Does the Applicant use third party or open source software code or software code? <input type="checkbox"/> Yes <input type="checkbox"/> No
With respect to software code supplied by a third party, does the Applicant require the third party to agree to any of the following? (Select all that apply)	
<input type="checkbox"/> Warranty against infringement	<input type="checkbox"/> Defend and indemnify the Applicant against infringement <input type="checkbox"/> Transfer of ownership or or assignment of license in all software code deliverables
Please describe the Applicant's processes for legal review and clearance of all third party and open source software code before use:	



11. MPL

Respond to the questions in this section only if applying for MPL coverage

11.1 Annual Gross Revenue (Professional Services):	Annual gross revenue derived from professional services projected for current fiscal year:	
	Annual gross revenue derived from professional services projected for next fiscal year:	
	Annual gross revenue derived from professional services for previous fiscal year:	
11.2 Client Engagements:	Provide the following for the Applicant's five largest client engagements, by the revenue derived from the engagement, during the last 5 years:	
	Client Name	Revenue
	1.	1.
	2.	2.
	3.	3.
	4.	4.
	5.	5.
11.3 Professional Services:	Please describe the professional services the Applicant provides that Applicant wishes to insure:	
11.4 Subcontractors:	Does the Applicant use subcontractors, independent contractors or other third party vendor to provide its professional services?	<input type="checkbox"/> Yes <input type="checkbox"/> No
	What percentage of the Applicant's professional services are provided by outsourcing?	
	Does the Applicant have standard written agreements with the vendors for all vendor services and products?	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Do the standard agreements include any of the following? (Select all that apply):	



AXIS CYBER TECHNOLOGY & MPL APPLICATION

<input type="checkbox"/> Transfer of ownership to the Applicant of all deliverables	<input type="checkbox"/> Require the vendor to defend and indemnify the Applicant against liability for harm caused by the vendor	
Are non standard agreements, or deviations from the standard agreement, reviewed by an attorney?		<input type="checkbox"/> Yes <input type="checkbox"/> No
11.5 Client Engagements:	Does the Applicant have standard written agreements with the vendors for all vendor services and products?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do the standard agreements include any of the following limitations of liability? Select all that apply:		
<input type="checkbox"/> Disclaimer of consequential or indirect damages	<input type="checkbox"/> Monetary cap on direct damages	
<input type="checkbox"/> Disclaimer of warranties		
What percentage of the Applicant's engagements are not subject to the standard agreement?		
Are non standard agreements, or deviations from the standard agreement, reviewed by an attorney?		<input type="checkbox"/> Yes <input type="checkbox"/> No
11.6 Project Management:	Does the Applicant have any of the following project management protocols and procedures, in writing? Select all that apply:	
<input type="checkbox"/> Scope of work, specifications, requirements and deliverables	<input type="checkbox"/> Customer acceptance signoff process	
<input type="checkbox"/> Timeline and milestones and milestone review process	<input type="checkbox"/> Complaint resolution or escalation process	
<input type="checkbox"/> Change order process		

12. CLAIMS AND EVENTS

12.1 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)	<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe:		
12.2 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)	<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe:		



AXIS CYBER TECHNOLOGY & MPL APPLICATION

<p>12.3 Unauthorized Access:</p>	<p>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)</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>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?</p>		<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Please describe:</p>		
<p>12.4 Prior Privacy Regulatory Actions:</p>	<p>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?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Please describe:</p>		
<p>12.5 Prior Claims:</p>	<p>During the last 3 years, has the Applicant received notice of any claim, complaint or demand alleging or arising out of liability that may trigger any insurance applied for herein?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Please describe:</p>		
<p>12.6 Prior Knowledge:</p>	<p>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 that may trigger any insurance applied for herein?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Please describe:</p>		
<p>12.7 Prior Notice:</p>	<p>Have any of these matters been reported to another insurer?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>12.8 Remediation:</p>	<p>In response to any of these matters, has the Applicant commenced or completed any change to remediate the circumstances that gave rise to the matter?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Please describe:</p>		



13. OTHER INSURANCE

13.1 Other Insurance:		Provide the following for each cyber or liability insurance policy carried by the Applicant during the last 5 years:		
Type of insurance	Policy limit	Retention or deductible	Policy period	Premium

14. 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.



AXIS CYBER TECHNOLOGY & MPL APPLICATION

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: _____



AXIS CYBER TECHNOLOGY & MPL APPLICATION

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 Division of Insurance within the Colorado 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.



AXIS CYBER TECHNOLOGY & MPL APPLICATION

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.



AXIS CYBER TECHNOLOGY & MPL APPLICATION

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.



AXIS CYBER TECHNOLOGY & MPL APPLICATION

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.