AXIS CYBER TECHNOLOGY & MPL APPLICATION

AXIS Specialty Europe SE Mount Herbert Court 34 Upper Mount Street Dublin 2 Ireland	AXIS Specialty London 52 Lime Street London EC3M 7AF	AXIS Managing Agency Ltd 52 Lime Street London EC3M 7AF

https://www.axiscapital.com/londonmarket/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

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: % Canada: % UK:	% Europe: % AUS/NZ: % LATAM:
			% MEA: % APAC: % Russia:
For how many years has the Applicant been in business?		☐ > 5 years ☐ 3-5 years	☐ 1-3 years ☐ < 1 year
Ownership Structure:	Category best describing ownership structure: (Select all that apply)	☐ Private ☐ Publicly traded ☐ Subsidiary ☐ Non-profit ☐ 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?	☐ Yes ☐ 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?		☐ Yes ☐ No
Does the Applicant store or process Personal Information on behalf of a third party?		☐ Yes ☐ 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?		☐ Yes ☐ 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)	☐ Web applications ☐ Hosted applications ☐ Removable media (USBs, offline storage) ☐ POS systems ☐ Vehicular onboard systems ☐ BYOD devices	☐ Terminals (ATMs) ☐ Healthcare devices ☐ Personal devices ☐ Critical IoT (Security, fire, BAS) ☐ AI/robotic devices ☐ OT/ICS/SCADA

How many servers are on the Applicant's network?	**On/Prem/Data Center:**	**Cloud:**	
Where are the servers located? (Select all that apply)	☐ US ☐ Canada ☐ UK	☐ Europe ☐ LATAM ☐ MEA	☐ AUS/NZ ☐ APAC ☐ 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?	☐ In-house ☐ Outsourced	
Do contractors or service providers have administrator privileges on the website?		☐ Yes ☐ 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?		☐ Yes ☐ No	
To whom does this role report? (Select all that apply)	☐ Executive committee or officers ☐ Principal owners or shareholders ☐ Board of directors	☐ CIO/CTO ☐ CFO ☐ CEO	☐ Other:
How frequently is a formal reporting provided?	☐ Monthly ☐ Quarterly	☐ Semi-annually ☐ Annually	☐ Ad Hoc ☐ Other:
Does the Applicant have a written information security policy?	☐ Yes ☐ No	Last updated:	
Identify any standards or frameworks the security program is based on: (Select all that apply)	☐ NIST CSF, 800-53, 171 or others ☐ ISO/IEC 27001 ☐ PCI-DSS	☐ CIS 18 ☐ 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?		☐ Yes ☐ No	
Security Management: Are any of the following implemented? (Select all that apply)	☐ Independent security audit/assessment ☐ Managed security services ☐ Unified threat mgt./prevention systems		
Screening: Are Applicants screened, including credit history, criminal, drug testing as permitted by law?		☐ Yes ☐ No	
The Applicant maintains the following documents:			

☐ Business Continuity Plan	Reviewed and tested	☐ Semi-annually ☐ Annually ☐ Other:
☐ Disaster Recovery Plan	Reviewed and tested	☐ Semi-annually ☐ Annually ☐ Other:
☐ Incident Response Plan	Reviewed and tested	☐ Semi-annually ☐ Annually ☐ Other:

Are copies of the above stored and accessible even if the network is unavailable?	☐ Yes ☐ No
Identify IR playbooks in place and tested:	☐ None ☐ Ransomware ☐ Business Email Compromise ☐ 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?			☐ Yes ☐ No
To whom does this role report? (Select all that apply)	☐ Executive committee or officers ☐ Principal owners or shareholders		☐ Board of directors ☐Other:
How frequently is a formal reporting provided?	☐ Monthly ☐ Quarterly	☐ Semi-annually ☐ Annually	☐ Ad Hoc ☐Other:
Does the Applicant have a written privacy policy or notice?	☐ Yes ☐ No	Last reviewed by attorney:	
Does the organization have user preference/behavior tracking functionality on their website?			☐ Yes ☐ No
This data is:	☐ Provided to a 3rd party or ☐ Maintained in house?		
Are contractual provisions in place that detail what data will be collected?			☐ Yes ☐ No
If a 3rd party, has a code review been performed to ensure only agreed data is transmitted?			☐ Yes ☐ No
Is Meta/Facebook or Google analytics providing this service?			☐ Yes ☐ No

3.3 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 (PI) subjected to the following activities during the last 12 months? (Select all that apply)	☐ Collection ☐ Sale ☐ Processing ☐ Deletion ☐ Sharing	
Can the Applicant identify the **source(s)** where PI is collected, sold, or shared?		☐ Yes ☐ No
Can the Applicant identify the **business purpose(s)** for which PI was collected, sold, or shared?		☐ Yes ☐ 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?	☐ GDPR ☐ GLBA ☐ CCPA ☐ PIPEDA	☐ TCPA ☐ BIPA ☐ VPPA ☐ CAN-SPAM	☐ FCRA/FACTA/Red Flags Rules ☐ Other:

Additional Comments:

4.2 Information Handling:

Identify disclosures made with respect to PI:

☐ **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.
☐ **Public notice** describing collection, sharing, sale and use.
☐ **Individual notice** at collection describing sharing, sale, and use.

Identify the processes in place for PI collected, shared, or sold: (Select all that apply)

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

Does the Applicant collect Biometric Information **(BI)**?	☐ Employees/contractors ☐ Customers	☐ Not collected ☐ 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)	☐ Cloud ☐ Applicant's network ☐ Other:	
Is BI subject to the following? (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 across borders to another jurisdiction?				☐ Yes ☐ No
Is the Applicant compliant with all laws pertaining to cross border transmission of PI?				☐ Yes ☐ No
4.3 PCI:	Is the Applicant required to be PCI-DSS compliant?			☐ Yes ☐ No
Is the Applicant PCI compliant?	☐ Yes ☐ No	Est. # of annual PCI transactions?		Merchant Level:
Is a payment processor used?	☐ Yes ☐ No	Are they assessed for PCI compliance annually?		☐ Yes ☐ No
Identify additional PCI controls:	☐ P2PE ☐ Tokenization ☐ Key storage off client network ☐ PCI training to critical staff			
Is Applicant required to be HIPAA compliant?	☐ Yes ☐ No	Is Applicant HIPAA compliant?		☐ Yes ☐ No
Additional Comments:				

5. CONTROLS

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

Indicate frequency of **external scanning**:	☐ Continuously ☐ Daily	☐ Weekly ☐ Monthly	☐ Quarterly ☐ Twice/yr.	☐ Annually ☐ Ad Hoc	☐ Never ☐ 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):					

5.2 Pen Testing:	The Applicant conducts regular penetration testing? (Select all that apply and frequency below) ☐ No
☐ External-network ☐ Internal-network ☐ Social engineering ☐ Physical ☐ Web App. ☐ Other:	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐Never ☐Other: ☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐Never ☐Other: ☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐Never ☐Other: ☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐Never ☐Other: ☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐Never ☐Other: ☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐Never ☐Other:
Testing is conducted:	☐ Internally ☐ Outsourced
Additional Comments:	

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?	☐ Yes ☐ No
If "Yes", please identify the EoL component(s):	If "Yes", please identify their function:	
Please indicate the controls applied to EoL components:	☐ Known and Inventoried ☐ Decomm/replacement plans in place ☐ Additional service purchased	☐ Tracked and reported ☐ Monitoring and alerting ☐ Segmented ☐ Other:
Are ALL EoL components covered by controls above:	☐ All covered ☐ Some not covered (Please provide detail in Additional Comments below)	
An up-to-date hardware and software inventory is maintained?	☐ Yes ☐ No	
Inventory processes are:	☐ Manual ☐ Semi-automated ☐ Fully automated	
Hardware inventory updates occur:	☐ Continuously ☐ 2x/yr. ☐ Other: ☐ Quarterly ☐ Annually	Percentage of hardware inventoried: %

Percentage of software inventoried?	%	Are users allowed to install applications?	☐ Yes ☐ No
Additional Comments:			

5.4 SOC/SIEM:	Does the Applicant use a SIEM?	☐ Yes (If yes, please identify the solution): ☐ No (Please provide detail in Additional Comments below)		
Is the SIEM tuned for your org. with 100% network log coverage?	☐ Yes ☐ No	If any, identify systems whose logs are excluded from SIEM:		
How frequently are logs reviewed?	☐ Continuously ☐ Weekly ☐ Monthly	☐ Quarterly ☐ Semi-annually ☐ Annually	How long are audit logs maintained? At least:	☐ 30 days ☐ 90 days ☐ 1 year or greater
Is a Security Operations Center (SOC) used?	☐ Yes ☐ No	If yes: ☐ Staffed 24/7/365 "eyes on glass" ☐ Other: ☐ Internal staff ☐ External staff ☐ SOC staff can take responsive or corrective action in event of alert.		
If 3rd 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:		
	☐ Laptops ☐ Workstations ☐ Mobile devices ☐ Web apps	☐ Servers ☐ Databases ☐ Security applications	☐ Not used ☐ Other:
Security configurations are updated at least:	☐ Monthly ☐Quarterly	☐ Semi-annually ☐ Annually	☐ Other:
Indicate hardening standards used:	☐ Center for Internet Security ☐ Microsoft ☐ NIST ☐ SANS ☐ Other:		
Additional Comments:			

Is software installation automatically controlled and unauthorized software blocked?	☐ Yes ☐ No

5.6 Backups & Redundancy:	Critical back-ups are completed:	☐ Continuously ☐ Weekly ☐ Other: ☐ Daily ☐ Monthly
Which of the following does the Applicant utilize for backups?		☐ Tapes ☐ Cloud ☐ Disk ☐ Other:
Back-ups are stored:		☐ On premises ☐ Offline ☐ Offsite ☐ Secondary Data Center ☐ MSSP ☐ Other:

Indicate existing backup controls:	☐ Segmentation ☐ Malware Scanning ☐ Unique Backup Accounts (stored separately) ☐ Encryption ☐ Immutable ☐ Priv. Access Mgt. ☐ Other:		
If encrypted, are keys stored offline?	☐ No ☐ Yes	If offline, how often is data moved?	☐Continuously ☐ Weekly ☐ Quarterly ☐ Daily ☐ Monthly ☐ Other:
Full, or large scale, restoration is tested:	☐ Quarterly ☐ Twice annually ☐ Annually ☐ Not tested ☐ Other:		
Identify redundancy or resiliency solutions in place:	☐ Hot Site ☐ Warm Site ☐ Snapshots ☐ Failover environment ☐ Other:		
Additional Comments:			

5.7 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 ☐ Bi-weekly ☐ Monthly ☐ 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?		☐ Yes ☐ 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?	☐ Yes ☐ No	Is DDoS mitigation in place?	☐ Yes ☐ No

5.9 Data Loss Prevention (DLP):	Does the Applicant employ a DLP solution?	☐ Yes ☐ 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?	☐ Off network ☐ Email ☐ Removable media ☐ Internet/Cloud (data storage sites, message boards, etc.)	
Are removable storage devices monitored and regulated?		☐ Yes ☐ No
Are data threshold alerts in place (exfiltration, deletion, movement)?		☐ Yes ☐ No

5.10 Encryption:	Does the Applicant employ mandatory encryption to protect the following? (Select all that apply)		
☐ Information in transit ☐ Information at rest	☐ Corporate Information at rest ☐ Corporate Information in transit	☐ Critical Information ☐ Removable media	☐ Personal devices ☐ Other:
5.11 Email Security:	Please identify the email security controls in place:		

☐ DKIM ☐ DMARC ☐ SPF	☐ Quarantine ☐ Block suspicous senders? ☐ Block malware/phishing/SPAM?	☐ Tag/notify external email ☐ Block malicious attachments/content? ☐ Macros disabled	☐ Sandboxing ☐ Other:

Does the Applicant employ Microsoft (Office) 365?	☐ Yes ☐ No	If yes, is MS365 ATP/Defender used? If yes, what is your MS Secure Score %?	☐ Yes ☐ No
If other cloud-based email/controls, please identify:			

Additional Comments:

5.12 Firewalls:	Does the Applicant employ the following firewalls?	☐ External or perimeter ☐ Internal
	Are default passwords changed?	☐ 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 restrictions, configurations, etc. are verified:	☐ Semi-annually ☐ Annually ☐ Ad Hoc ☐ Other:
What is the firewall policy? (Select all that apply)	☐ Deny all by default, permit by exception ☐ Deny by exception ☐ Other:

Additional Comments:

5.13 Segmentation:	Are the following segregated in an isolated environment?	☐ Personal Information ☐ Critical servers	☐ Corporate Information ☐ Critical Information
Indicate any existing network segmentation:	☐ Geographic ☐ IT Management ☐ Business Function ☐ Subsidiaries	☐ Guest wireless ☐ Servers ☐ OT ☐ None	☐ Other:
How is segmentation accomplished?	☐ Firewalls ☐ Sep. Domains ☐ VLAN's ☐ Other (Please provide detail in Additional Comments below)		
Are development, testing and production conducted in separate environments?	☐ Yes ☐ No		

Additional Comments:

5.14 Access:	Is network and information access based on a least privilege basis?	☐ Yes ☐ No
Is a formal process in place for assigning access for all hires, terms, and changes?	☐ Yes ☐ No	If "Yes", is it: ☐ Manual ☐ Semi-automated ☐ Fully automated ☐ Other:
User access is reviewed and updated:	☐ Monthly ☐ Quarterly ☐ Annually ☐ Never ☐ Other:	

Admin/privileged access is reviewed & updated:	☐ Monthly ☐ Quarterly ☐ Annually ☐ Never ☐ Other:

Does the Applicant impose minimum security requirements on all devices connecting to the network?	☐ Yes ☐ No
Does the Applicant use a Mobile Device management (MDM) solution that allows remote wipe?	☐ Yes ☐ No

Passwords: Please identify any required password elements:	☐ Min. char. length 10 or > ☐ Min. char. length 9 or < ☐ Upper/Lower/Special char.	☐ Expiration every 6 months or less ☐ Check for cracked/common passwords ☐ Lockout after 6 invalid attempts	☐ Dictionary check ☐ Passphrase ☐ Other:

Additional Information:

5.15 Domain/ Privileged Accounts & Controls:	Please identify domain admin/priv. account controls in place?	☐ Separate accts. ☐ PAM/Pwd vault ☐ PAM (Check In/Out) ☐ Priv. Access Workstations	☐ Other:

If PAM or Vault:	• Is a separate MFA instance required to access this? • Are all domain admin accounts (incl. service accounts) maintained in the solution?	☐ Yes ☐ No ☐ Yes ☐ 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?	☐ Yes ☐ No
Are changes to admin/privileged accounts monitored and alerted automatically?	☐ Yes ☐ No
All service accts have interactive login disabled?	☐ Yes ☐ 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):	☐ None ☐ Limited # of users ☐ Other: ☐ All ☐ LAPS or similar control in place ☐ 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)

☐ All Admin/Privileged access (On-prem AND remote) ☐ All access to cloud-based solutions ☐ All remote access into network ☐ Remote access by vendors/contractors	☐ Access to backups ☐ Access to Remote Desktop Protocol or similar ☐ Access to cloud email (i.e.:MS365) ☐ Other:

What MFA methods are in use?	☐ Secondary Email ☐ SMS/Text ☐ Biometrics	☐ Authenticator App ☐ Physical keyfob/card ☐ Other:	☐ Endpoint Cert.(Please indicate where used):
Additional Comments:			

Wireless:	Does the Applicant maintain wireless security policies:	☐ Yes ☐ No	
Are connections from untrusted wireless devices allowed?	☐ Yes ☐ No	If, yes, do untrusted wireless devices use a separate network?	☐ Yes ☐ No

5.17 Training & Awareness:	Annual training is required for:	☐ Employees/Contractors ☐ Vendors ☐ Ad hoc only ☐ Not Required	Please indicate topics:	☐ Threats ☐ Privacy ☐ Social Eng. ☐ Regulations/Policy ☐ Role-based ☐ Data Handling ☐ Phishing ☐ Other:
Are Phishing simulations conducted for all employees?	☐ Yes ☐ No	If "Yes", indicate frequency:	☐ Monthly ☐ Twice Annually ☐ Ad Hoc ☐ Quarterly ☐ Annually ☐ Other:	
Are Phishing Simulations:	☐ Role Based ☐ Targeted ☐ Staggered			
What % of staff are covered in each simulation?	☐100% ☐25% or less ☐25 to 50% ☐50% to 75% ☐Other:			
Click rate of most recent simulation:	☐ <5% ☐5-10% ☐ 10-15% ☐15-20% ☐ >20% ☐Other:			
What is the most recent reporting rate?	☐ <5% ☐5-10% ☐ 10-15% ☐15-20% ☐ >20% ☐ Other:			

Does the Applicant require additional training on failure?	☐ Yes ☐ No
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
Is information security and privacy training content reviewed at least annually?	☐ Yes ☐ No
Are service providers/3rd parties with access to the network required to take this training annually?	☐ Yes ☐ No
Additional Comments:	

5.18 RDP/SMB	Is RDP or other remote connection solution enabled?	☐ Yes ☐ No

If "Yes", is RDP or other accessible:	☐ Internally ☐ Externally (public) ☐ External only after remote connection/VPN
Indicate additional controls:	☐ Restricted to IT personnel ☐ Sep. accounts required ☐ Network authentication ☐ Alerting and monitoring for each use ☐ Accessible through PAM ☐ Other: ☐ Lockout after failed attempts
Is SMB v.1 or v.2 available/in use on your network?	☐ Yes ☐ 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:	☐ < 8 hours ☐ 8-12 hours	☐ 12-24 hours ☐ 24-48 hours	☐ > 48 hours ☐ Other:
Have these been validated in the last 12 months?			☐ Yes ☐ 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:	☐ < 1 hour ☐ 1-8 hours	☐ 8-12 hours ☐ 12-24 hours	☐ 24-48 hours ☐ Other:
Does the Applicant have a manual workaround in the event of an interruption of the network?			☐ Yes ☐ No
Please describe:			
Does the Applicant have immediate failover capacity in the event of a critical network interruption?			☐ Yes ☐ No
Please describe:			
Does the Applicant maintain a hot, warm, or cold site backup IT facility?			☐ None ☐ Hot ☐ Warm ☐ Cold
Please describe:			

6.3 Incident Response:	Does the Applicant have a written Incident Response Plan (IRP) reviewed annually?	☐ Yes ☐ No
Does the Applicant have ransomware and/or other playbooks? Has the Applicant completed table-top or similar testing of the IRP in last 12 months?		☐ Yes ☐ No ☐ Yes ☐ No

Additional Comments:		
6.4 Prior Event:	Has the Applicant experienced a partial or total network interruption lasting more than 8 hours?	☐ Yes ☐ 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 Applicants 3rd party review process:	☐ Security Program ☐ In/External Audits ☐ Tech. changes	☐ Data provided to vendor ☐ Services and changes ☐ Leadership changes	☐ Periodic Review based on risk ☐ No Review process

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?	☐ Yes ☐ No	☐ Ad hoc ☐ During onboarding ☐ Risk-based	☐ Documented procedure ☐ On contract renewal ☐ Defined intervals

Is service provider access to the Applicant's network or data restricted on a least privilege basis?			☐ Yes ☐ No
Is service provider access to the Applicant's data or network reviewed?	☐ Yes (if "Yes", indicate frequency) ☐ No	☐ Continuously ☐ Monthly ☐ Quarterly	☐ Semi-annually ☐ Annually ☐ 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?	☐ Yes ☐ 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?		☐ 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:		

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?	☐ Yes ☐ No
Please describe:		
Does the Applicant employ a protocol requiring more than one or next-level approval?		☐ Yes ☐ No
Please describe:		

8.3 Anti-Fraud Training:	Does the Applicant conduct anti-fraud training of employees at least annually?	☐ Yes ☐ 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?	☐ Yes ☐ 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)	☐ Unlicensed third-party content (message boards, reviews) ☐ Content created by the Applicant ☐ Licensed third party content	☐ Streaming video or music content ☐ 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?	☐ 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 copyright, plagiarism or misappropriation of ideas ☐ 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?		☐ 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
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?	☐ 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:	

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	☐	%
Client relationships management (CRM) or enterprise risk management (ERM) or supply chain software	☐	%
Computer aided design, manufacturing or drafting (CAD/CAM)	☐	%

Data analytics or mining, processing, storage or encryption		☐	%
E-commerce service		☐	%
Electronic auction services		☐	%
Hardware – manufacturing and design of hardware, components and equipment		☐	%
Hardware – sales, installation and maintenance		☐	%
Information Technology (IT) – technical support, maintenance, testing or training, business process outsourcing		☐	%
Information Technology (IT) – systems analysis, design, engineering, audit, programming or implementation and related consulting		☐	%
Internet service provider (ISP), domain name services, search engine, email or instant messaging (IM)		☐	%
Internet media or online advertising or branding		☐	%
Managed network or security services or hosting, cloud or colocation		☐	%
Payment processing services		☐	%
Sale, lease or licensing of proprietary technology or telecommunications products to others		☐	%
Where is the proprietary technology hosted? Select all that apply	☐ Cloud hosted	☐ Client hosted	☐ 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)		☐	%
Software development and design – custom		☐	%
• Does the Applicant perform any integration of custom software into the client's network?		☐ Yes ☐ No	
Software development and design – packaged		☐	%
Web page development, design and related consulting		☐	%
Website hosting or administration or web portal services		☐	%
Other technology services or products. Please describe:		☐	%

10.4 Subcontractors:	Does the Applicant use subcontractors, independent contractors or other third party vendor to provide its technology services and products?	☐ Yes ☐ 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?		☐ Yes ☐ No
Do the standard agreements include any of the following? Select all that apply:		
☐ Transfer of ownership to the Applicant of all deliverables	☐ 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?		☐ Yes ☐ No
10.5 Client Engagements:	Does the Applicant have standard written agreements with clients for all technology services and products?	☐ Yes ☐ No
Do the standard agreements include any of the following limitations of liability? Select all that apply:		

☐ Disclaimer of consequential or indirect damages	☐ Monetary cap on direct damages
☐ 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?	☐ Yes ☐ No

10.6 Project Management:	Does the Applicant have any of the following project management protocols and procedures? (Select all that apply):	
☐ Scope of work, specifications, requirements and deliverables	☐ Customer acceptance signoff process	
☐ Timeline and milestones and milestone review process	☐ Complaint resolution or escalation process	
☐ 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:	
☐ Beta testing or user acceptance testing	☐ Written product recall process	
☐ Post project review process	☐ Vendor or VAR certification process	
☐ Client relationship management staff	☐ 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?	☐ Yes ☐ 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)		
☐ Warranty against infringement	☐ Defend and indemnify the Applicant against infringement	☐ 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?	☐ Yes ☐ 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?		☐ Yes ☐ No
Do the standard agreements include any of the following? (Select all that apply):		

☐ Transfer of ownership to the Applicant of all deliverables	☐ 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?	☐ Yes ☐ No

11.5 Client Engagements:	Does the Applicant have standard written agreements with the vendors for all vendor services and products?	☐ Yes ☐ No

Do the standard agreements include any of the following limitations of liability? Select all that apply:

☐ Disclaimer of consequential or indirect damages	☐ Monetary cap on direct damages
☐ 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?	☐ Yes ☐ No

11.6 Project Management:	Does the Applicant have any of the following project management protocols and procedures, in writing? Select all that apply:	

☐ Scope of work, specifications, requirements and deliverables	☐ Customer acceptance signoff process
☐ Timeline and milestones and milestone review process	☐ Complaint resolution or escalation process
☐ 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)	☐ Yes ☐ 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)	☐ Yes ☐ No
Please describe:		

12.3 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:		
12.4 Prior Privacy 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:		
12.5 Prior Claims:	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?	☐ Yes ☐ No
Please describe:		
12.6 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 that may trigger any insurance applied for herein?	☐ Yes ☐ No
Please describe:		
12.7 Prior Notice:	Have any of these matters been reported to another insurer?	☐ Yes ☐ No
12.8 Remediation:	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?	☐ Yes ☐ No
Please describe:		

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.

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 _____

Please view our Privacy Notice via this link:
https://www.axiscapital.com/canada/who-we-are/privacy-notice