# AXIS CYBER & TECHNOLOGY APPLICATION

**AXIS REINSURANCE COMPANY (CANADIAN BRANCH)**
70 YORK STREET SUITE 1010
TORONTO, ON M5J 1S9
Telephone**: (416) 361-7200** | Fax: **(416) 361-7225**

https://www.axiscapital.com/canada/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.**

## 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 applications for those.**
- This Application and all materials submitted herewith shall be held in confidence.
- The submission of this Application does not obligate the Applicant to buy insurance nor is the Insurer obligated to sell insurance or to offer insurance upon any specific terms requested.
- If the policy applied for is issued, this Application, which shall include all Supplemental Applications and material and information submitted in connection with this Application, will be deemed attached to and will form a part of the policy.

## INSTRUCTIONS

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

If space is insufficient, continue responses on your letterhead.

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

| **Section A: Applicant Information** | |
|---|---|
| **Applicant Name:** | |
| **Applicant Mailing Address:** | |

| | | | |
|---|---|---|---|
| **Website(s):** | | | |
| **Risk Manager Contact:** | | | |
| **Incident Response Contact:** | | | |
| **Business Activities:** | Please describe the Applicant's business activities, services and products | | |
| **Revenue:** | Annual gross revenue projected for current fiscal year | | |
| Annual gross revenue for previous fiscal year | | | |
| **Operating Cost:** | Annual operating cost for current fiscal year | | |
| Current fiscal year budget allocation to | IT: | Cybersecurity: | |
| **Headcount:** | Employees: | Contractors: | |
| | Working remotely: | | |
| **Regions:** | Percentage of projected revenue in US and outside the US: | % US | % Non US |

| **Section B: Data Assets** | |
|---|---|
| **Personal Information:** | For purposes of this application, Personal Information refers to PII, PHI, PCI and Biometric Information described below. |
| 1. With respect to each of the following types of Personal Information, what is the approximate number of unique individuals whose Personal Information is collected, stored, used or processed by the Applicant or by a third party on behalf of the applicant? | |

| | | |
|---|---|---|
| PII | Information from which an individual can be uniquely and reliably identified or contacted or that is used for authenticating an individual for business transactions or access to the individual's accounts or records.<br>(Individual's name, address, email address, telephone number, passport, social security, driver's license or other government issued identification numbers, credit, debit or other financial account numbers, security codes, passwords, PINs and security questions and answers) | |
| PHI | Individual's health or medical information<br>(Individual's name, medical records, medical history, medical bills, lab test results, medical record numbers, health plan or health beneficiary numbers, medical device identifiers and serial numbers) | |
| PCI | Payment card information | |
| Biometric | An individual's unique physical or behavioral characteristics.<br>(Fingerprints, faceprints, hand scans, vein patterns, voiceprints, iris or retina scans, keystroke, gait or other physical patterns, sleep/health/exercise data, DNA or biological markers) | |
| 2. Does the Applicant sell or share Personal Information? | | ☐ Yes ☐ No |
| 3. Does the Applicant store or process Personal Information on behalf of a third party? | | ☐ Yes ☐ No |
| **Corporate Information** | For purposes of this application, Corporate Information refers to third party IP, intangible assets, trade secrets, nonpublic business information, such as insider financial information, M&A and business or product development information, client lists, sales projections and strategy, or information that is marked "confidential". | |
| 4. Does the Applicant store or process Corporate Information? | | ☐ Yes ☐ No |

| **Section C: PCI DSS Compliance** | |
|---|---|
| 5. Is the Applicant required to be compliant with the PCI DSS? | ☐ Yes ☐ No |
| 6. PCI Merchant Level (1-4): | |
| 7. How many payment card transactions does the Applicant process annually? | |
| 8. Is the Applicant currently compliant with the PCI DSS requirements for its merchant level? | ☐ Yes ☐ No |
| 9. Which version of PCI-DSS was the Applicant assessed against? | |

| Section D: Governance | | | | |
|---|---|---|---|---|
| 10. Does the Applicant have a written privacy policy or privacy notice reviewed by an attorney and updated at least annually? | | | | ☐ Yes ☐ No |
| 11. Does the Applicant have a written information security policy? | | | | ☐ Yes ☐ No |
| 11a. When was this policy last updated? | | | | |
| 11b. Is it based on or aligned with any of the following standards, frameworks or best practices? Select all that apply | | | | |
| ☐ NIST Cybersecurity Framework or other publications | | ☐ ISO/IEC 27001 | ☐ US-CERT | |
| 12. Identify any other | | | | |
| 13a. Does the Applicant have a written business continuity plan? | | | | ☐ Yes ☐ No |
| 13b. How frequently is this plan tested? At least: | | ☐ Quarterly | ☐ Semi annually | ☐ Annually |
| 14a. Does the Applicant have a written disaster recovery plan? | | | | ☐ Yes ☐ No |
| 14b. How frequently is this plan tested? At least: | | ☐ Quarterly | ☐ Semi annually | ☐ Annually |
| 15a. Does the Applicant have a written incident response plan? | | | | ☐ Yes ☐ No |
| 15b. How frequently is this plan tested? At least: | | ☐ Quarterly | ☐ Semi annually | ☐ Annually |
| 16. Are copies of the business continuity/disaster recovery and incident response plans stored so that they will be accessible if the Applicant's network became completely unavailable? | | | | ☐ Yes ☐ No |
| 17a. Does the Applicant have a written document retention policy? | | | | ☐ Yes ☐ No |
| 17b. Does the Applicant have a written recordkeeping policy? | | | | ☐ Yes ☐ No |
| 17c. Do these policies enable the Applicant to identify all Personal Information subjected to the following activities during the last 12 months? Select all that apply | | | | |
| ☐ Collection | ☐ Processing | ☐ Sharing | ☐ Sale | ☐ Deletion |
| 17d. Do these policies enable the Applicant to identify the source(s) from which Personal Information was collected, sold or shared? | | | | ☐ Yes ☐ No |

| | |
|---|---|
| 17e. Do these policies enable the Applicant to identify the business purpose(s) for which Personal Information was collected, sold or shared? | ☐ Yes ☐ No |

| **Section E: Controls** | | | | |
|---|---|---|---|---|
| 18. Does the Applicant employ any Intrusion Detection and Prevention solutions (IDP), e.g. anti-virus software? | | | | ☐ Yes ☐ No |
| 19a. Is Remote Desktop Protocol (RDP) enabled? *If yes, complete 19b* | | | | ☐ Yes ☐ No |
| 19b. Is RDP accessible externally? *If yes, complete 19c* | | | | ☐ Yes ☐ No |
| 19c. Is Multi Factor Authentication used for access? | | | | ☐ Yes ☐ No |
| 20a. If remote access is available, does the Applicant implement MFA for all remote access? | | | | ☐ Yes ☐ No ☐ N/A |
| 20b. Does the Applicant or its Managed Security Service Provider, if applicable, implement MFA for all administrator access? | | | | ☐ Yes ☐ No |
| 21. What is the Applicant's Critical Patching Target? | | | | |
| ☐ < 24 Hours | ☐ 1 – 7 Days | ☐ 8 – 14 Days | ☐ 15 – 30 Days | ☐ > 30 Days |
| 22. Does the Applicant employ an Endpoint Detection and Response solution (EDR) that covers 100% of its environment? (For example, CrowdStrike, Carbon Black or similar solution) | | | | ☐ Yes ☐ No |
| 23. Does the Applicant employ any of the following solutions? | | SPF ☐ Yes ☐ No | DKIM ☐ Yes ☐ No | DMARC ☐ Yes ☐ No |
| 24. Does the Applicant maintain a Normal Vulnerability Management patching target within 30 days? | | | | ☐ Yes ☐ No |
| 25a. Does the Applicant have a Security Operations Center (SOC) or utilize a Managed Security Service Provider? | | | | ☐ Yes ☐ No |
| 25b. If yes, is it monitored 24/7? | | | | ☐ Yes ☐ No |
| 26a. Does the Applicant have any End-of-Life software or systems present in its environment? | | | | ☐ Yes ☐ No |
| 26b. If yes, please indicate additional controls in place to secure these: | | | | |
| Extended support purchased ☐ Yes ☐ No | Systems segmented ☐ Yes ☐ No | Application Whitelisting enabled ☐ Yes ☐ No | | Internet access disabled ☐ Yes ☐ No |
| 27a. Please describe the Applicant's audit logging policies, anomaly review practices and log analysis solutions, such as SIEM. | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 27b. Are these policies, practices and solutions applied to the following? Select all that apply | | | ☐ Firewalls | ☐ Intrusion detection and prevention |
| 27c. Is the local logging performed on a per-host basis? | | | | ☐ Yes ☐ No |
| 27d. Are local logs centralized into a log management system? | | | | ☐ Yes ☐ No |
| 27e. How frequently are logs audited? At least: | | | | ☐ Continuously |
| ☐ Weekly | ☐ Monthly | ☐ Quarterly | ☐ Semi annually | ☑ Annually |
| 27f. How long are audit logs maintained? At least: | | ☐ 30 days | ☐ 90 days | ☐ 1 year |
| 28. Does the Applicant employ mandatory encryption to protect the following? Select all that apply | | | | |
| ☐ Personal Information in transit | | ☐ Personal Information at rest | | |
| ☐ Corporate Information in transit | | ☐ Corporate Information at rest | | |
| ☐ Critical Information | ☐ Personal devices | ☐ Removable media | | |

| **Section F: Training & Awareness** | |
|---|---|
| 29. Does the Applicant conduct mandatory information security, phishing and privacy training for employees and contractors at least quarterly? | ☐ Yes ☐ No |
| 30. Are Phishing Simulations conducted for all employees? | ☐ Yes ☐ No |
| 31. Does the Applicant have a report phishing email add-in enabled for all email users? | ☐ Yes ☐ No |
| 32. Does the Applicant employ a sandboxing solution for investigating suspicious emails/attachments | ☐ Yes ☐ No |

| **Section G: Backups** | | | | |
|---|---|---|---|---|
| 33. Does the Applicant conduct regular backup of data? | | | | ☐ Yes ☐ No |
| 34. Is Critical Information backed up at least? | | | | |
| ☐ Daily | ☐ Weekly | ☐ Monthly | ☐ Quarterly | ☐ > Semi-Annually |
| 35. Which of the following does the Applicant utilize for backups? Select all that apply | | Tapes ☐ Yes ☐ No | Disks ☐ Yes ☐ No | Cloud ☐ Yes ☐ No |
| 36. Where are backups stored? Select all that apply | | | | |
| Managed Security Service Provider ☐ Yes ☐ No | On premises ☐ Yes ☐ No | Offline storage ☐ Yes ☐ No | Offsite storage ☐ Yes ☐ No | Secondary data center ☐ Yes ☐ No |

| 37. Are backups subject to the following measures? Select all that apply | | | | |
|---|---|---|---|---|
| Multi Factor Authentication<br>☐ Yes ☐ No | Encryption<br>☐ Yes ☐ No | Segmentation<br>☐ Yes ☐ No | Virus/malware scanning<br>☐ Yes ☐ No | Immutable<br>☐ Yes ☐ No |

| | | | | |
|---|---|---|---|---|
| 38. Are unique backup credentials stored separately from other user credentials | | | | ☐ Yes ☐ No |
| 39. Backups are made to offsite or offline storage at least: | ☐ Daily | ☐ Weekly | ☐ Monthly | ☐ Quarterly |
| 40. Is full recovery from a backup tested at least annually? | | | | ☐ Yes ☐ No |

## Section H: Recovery Time & Impact

| 41. In the event of an interruption of the Applicant's network, at most how long is the Applicant's recovery time objective (RTO) for critical systems, applications, and processes? | | | | |
|---|---|---|---|---|
| ☐ < 1 day | ☐ 1-2 days | ☐ 3-5 days | ☐ 6-10 days | ☐ > 10 days |
| 42. Has the Applicant's RTO been validated in the last 12 months? | | | | ☐ Yes ☐ No |
| 43. In the event Critical Information, or critical systems, applications or processes became unavailable, at most how long would it take to materially interrupt the Applicant's business? | | | | |
| ☐ < 1 hour | ☐ 1-8 hours | ☐ 8-12 hours | ☐ 12-24 hours | ☐ 24-48 hours |

## Section I: Biometric Information

| | |
|---|---|
| 44. Does the Applicant, or any third party acting on the Applicant's behalf, collect, use, process, share, sell, profit from or retain Biometric Information. Biometric Information means individual's unique physical or behavioral characteristics (fingerprints, faceprints, hand scans, vein patterns, voiceprints, iris or retina scans, keystroke, gait or other physical patterns, sleep/health/exercise data, DNA or biological markers). | ☐ Yes ☐ No |
| 45. Are any of the Applicant's products or services used in the collection, use, processing, sharing, sale, profit from, possession, retention and destruction of Biometric Information? | ☐ Yes ☐ No |

## Section J: Crime

| | |
|---|---|
| 46. What is the daily average number of transactions transferring first party funds? | |
| 47. What is the average value transferred each day? | |
| 48. What is the average value of any one transfer? | |
| 49a. 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 |

| | |
|---|---|
| 49b. Please describe | |
| 50a. Does the Applicant employ a protocol requiring more than one or next-level approval? | ☐ Yes ☐ No |
| 50b. Please describe | |
| 51. Does the Applicant conduct anti-fraud training of employees at least annually? | ☐ Yes ☐ No |
| 52a. 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 |
| 52b. Please describe | |

| **Section K: Media** | |
|---|---|
| 53. Please describe the Applicant's media activities including advertising activities | |
| | |
| 54. Current fiscal year budget allocation to advertising activities: | |

| | | | |
|---|---|---|---|
| 55. What type of content does the Applicant publish or post on its website?<br>Select all that apply | | | ☐ No website |
| ☐ Content created by the Applicant | ☐ Licensed third party content | ☐ Unlicensed third party content (message boards, reviews) | ☐ Streaming video or music content |
| 56a. 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 |
| 56b. Does the attorney's review screen for the following liability risks? Select all that apply | | | |
| ☐ Defamation or disparagement | ☐ Outrage or infliction of emotional distress | ☐ Infringement of privacy or publicity rights | ☐ Infringement of copyright, plagiarism or misappropriation of ideas |
| 57. 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 |
| 58. Does the Applicant have a written policy for handling requests for retractions or corrections? | | | ☐ Yes ☐ No |
| 59. 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 |
| 60a. 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 |
| 60b. 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 |
| 60c. 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 |
| 60d. Do any of the written agreements limit the third party's liability arising out of the third party's services or content? | | | ☐ Yes ☐ No |

## Section L: Security and Privacy Claims and Events

| | |
|---|---|
| 61. 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?<br>(damage to, destruction, loss, theft, unauthorized disclosure) | ☐ Yes ☐ No |

| | |
|---|---|
| 62. 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?<br>(wrongful collection, retention, sale, disposal, deletion, disclosure, use, control, processing, access or correction) | ☐ Yes ☐ No |
| 63. During the last 3 years, has the Applicant experienced any failure of the security of its network?<br>(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 |
| 64. 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 |
| 65. 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 |
| 66. Does any director, officer or employee of the Applicant, its parent company or any of its subsidiaries or affiliates have knowledge or information about any fact, circumstances, incident, event or transaction that may give rise to a claim, complaint or demand alleging a privacy or security incident or media liability? | ☐ Yes ☐ No |
| 67. Have any of these matters been reported to another insurer? | ☐ Yes ☐ No |
| 68. In response to any of these matters, has the Applicant commenced or completed any change to its network and information security and handling practices, or other changes, to remediate the effects of the matter or remove a vulnerability that gave rise to the matter? | ☐ Yes ☐ No |
| 69. Please describe Security and Privacy Claims and Events (if any): | |

## REPRESENTATIONS AND SIGNATURE

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

1. The statements and answers given in and all materials submitted with this Application are true, accurate and complete.
2. No facts or information material to the risk proposed for insurance have been misstated or concealed.
3. These representations are a material inducement to the Insurer to provide a proposal for insurance.

4. Any policy the Insurer issues will be issued in reliance upon these representations.

5. The Applicant will report to the Insurer immediately in writing any material change in the Applicant's activities, products and services.

6. The Applicant will report to the Insurer immediately in writing any material changes to the answers provided in this Application which occur or are discovered between the date of this Application and the effective date of the policy for which coverage is sought by submission this Application.

7. The Insurer reserves the right, upon receipt of any such notice, to modify or withdraw any proposal for insurance the Insurer has offered.

WARNING

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 _____