



AXIS CYBER APPLICATION FOR SMALL BUSINESS

AXIS INSURANCE

111 S. Wacker Dr., Ste. 3500

Chicago, IL 60606

Telephone: (678) 746-9000 | Toll-Free: (866) 259-5435 | Fax: (678) 746-9315

<https://www.axiscapital.com/insurance/cyber-technology-e-o>

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

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:	



AXIS CYBER APPLICATION FOR SMALL BUSINESS

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?			



AXIS CYBER APPLICATION FOR SMALL BUSINESS

PII	Information from which an individual can be uniquely and reliably identified or contacted or that is used for authenticating an individual for business transactions or access to the individual's accounts or records. (Individual's name, address, email address, telephone number, passport, social security, driver's license or other government issued identification numbers, credit, debit or other financial account numbers, security codes, passwords, PINs and security questions and answers)	
PHI	Individual's health or medical information (Individual's name, medical records, medical history, medical bills, lab test results, medical record numbers, health plan or health beneficiary numbers, medical device identifiers and serial numbers)	
PCI	Payment card information	
Biometric	An individual's unique physical or behavioral characteristics. (Fingerprints, faceprints, hand scans, vein patterns, voiceprints, iris or retina scans, keystroke, gait or other physical patterns, sleep/health/exercise data, DNA or biological markers)	
2. Does the Applicant sell or share Personal Information?		<input type="checkbox"/> Yes <input type="checkbox"/> No
3. Does the Applicant store or process Personal Information on behalf of a third party?		<input type="checkbox"/> Yes <input type="checkbox"/> 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?		<input type="checkbox"/> Yes <input type="checkbox"/> No

Section C: PCI DSS Compliance

5. Is the Applicant required to be compliant with the PCI DSS?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9. Which version of PCI-DSS was the Applicant assessed against?	



AXIS CYBER APPLICATION FOR SMALL BUSINESS

Section D: Governance

10. Does the Applicant have a written privacy policy or privacy notice reviewed by an attorney and updated at least annually?				<input type="checkbox"/> Yes <input type="checkbox"/> No
11. Does the Applicant have a written information security policy?				<input type="checkbox"/> Yes <input type="checkbox"/> 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				
<input type="checkbox"/> NIST Cybersecurity Framework or other publications	<input type="checkbox"/> ISO/IEC 27001	<input type="checkbox"/> US-CERT		
12. Identify any other				
13a. Does the Applicant have a written business continuity plan?				<input type="checkbox"/> Yes <input type="checkbox"/> No
13b. How frequently is this plan tested? At least:	<input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi annually	<input type="checkbox"/> Annually	
14a. Does the Applicant have a written disaster recovery plan?				<input type="checkbox"/> Yes <input type="checkbox"/> No
14b. How frequently is this plan tested? At least:	<input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi annually	<input type="checkbox"/> Annually	
15a. Does the Applicant have a written incident response plan?				<input type="checkbox"/> Yes <input type="checkbox"/> No
15b. How frequently is this plan tested? At least:	<input type="checkbox"/> Quarterly	<input type="checkbox"/> Semi annually	<input type="checkbox"/> 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?				<input type="checkbox"/> Yes <input type="checkbox"/> No
17a. Does the Applicant have a written document retention policy?				<input type="checkbox"/> Yes <input type="checkbox"/> No
17b. Does the Applicant have a written recordkeeping policy?				<input type="checkbox"/> Yes <input type="checkbox"/> 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				
<input type="checkbox"/> Collection	<input type="checkbox"/> Processing	<input type="checkbox"/> Sharing	<input type="checkbox"/> Sale	<input type="checkbox"/> Deletion
17d. Do these policies enable the Applicant to identify the source(s) from which Personal Information was collected, sold or shared?				<input type="checkbox"/> Yes <input type="checkbox"/> No



AXIS CYBER APPLICATION FOR SMALL BUSINESS

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.



AXIS CYBER APPLICATION FOR SMALL BUSINESS

27b. Are these policies, practices and solutions applied to the following? Select all that apply		<input type="checkbox"/> Firewalls		<input type="checkbox"/> Intrusion detection and prevention
27c. Is the local logging performed on a per-host basis?				<input type="checkbox"/> Yes <input type="checkbox"/> No
27d. Are local logs centralized into a log management system?				<input type="checkbox"/> Yes <input type="checkbox"/> No
27e. How frequently are logs audited? At least:				<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
27f. How long are audit logs maintained? At least:		<input type="checkbox"/> 30 days	<input type="checkbox"/> 90 days	<input type="checkbox"/> 1 year
28. Does the Applicant employ mandatory encryption to protect the following? Select all that apply				
<input type="checkbox"/> Personal Information in transit		<input type="checkbox"/> Personal Information at rest		
<input type="checkbox"/> Corporate Information in transit		<input type="checkbox"/> Corporate Information at rest		
<input type="checkbox"/> Critical Information	<input type="checkbox"/> Personal devices	<input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
30. Are Phishing Simulations conducted for all employees?	<input type="checkbox"/> Yes <input type="checkbox"/> No
31. Does the Applicant have a report phishing email add-in enabled for all email users?	<input type="checkbox"/> Yes <input type="checkbox"/> No
32. Does the Applicant employ a sandboxing solution for investigating suspicious emails/attachments	<input type="checkbox"/> Yes <input type="checkbox"/> No

Section G: Backups

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



AXIS CYBER APPLICATION FOR SMALL BUSINESS

37. Are backups subject to the following measures? Select all that apply				
Multi Factor Authentication <input type="checkbox"/> Yes <input type="checkbox"/> No	Encryption <input type="checkbox"/> Yes <input type="checkbox"/> No	Segmentation <input type="checkbox"/> Yes <input type="checkbox"/> No	Virus/malware scanning <input type="checkbox"/> Yes <input type="checkbox"/> No	Immutable <input type="checkbox"/> Yes <input type="checkbox"/> No
38. Are unique backup credentials stored separately from other user credentials				<input type="checkbox"/> Yes <input type="checkbox"/> No
39. Backups are made to offsite or offline storage at least:	<input type="checkbox"/> Daily	<input type="checkbox"/> Weekly	<input type="checkbox"/> Monthly	<input type="checkbox"/> Quarterly
40. Is full recovery from a backup tested at least annually?				<input type="checkbox"/> Yes <input type="checkbox"/> 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?				
<input type="checkbox"/> < 1 day	<input type="checkbox"/> 1-2 days	<input type="checkbox"/> 3-5 days	<input type="checkbox"/> 6-10 days	<input type="checkbox"/> > 10 days
42. Has the Applicant's RTO been validated in the last 12 months?				<input type="checkbox"/> Yes <input type="checkbox"/> 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?				
<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

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).	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No



AXIS CYBER APPLICATION FOR SMALL BUSINESS

49b. Please describe		
50a. Does the Applicant employ a protocol requiring more than one or next-level approval?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
50b. Please describe		
51. Does the Applicant conduct anti-fraud training of employees at least annually?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> 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:	



AXIS CYBER APPLICATION FOR SMALL BUSINESS

55. What type of content does the Applicant publish or post on its website? Select all that apply			<input type="checkbox"/> No website
<input type="checkbox"/> Content created by the Applicant	<input type="checkbox"/> Licensed third party content	<input type="checkbox"/> Unlicensed third party content (message boards, reviews)	<input type="checkbox"/> 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?			<input type="checkbox"/> Yes <input type="checkbox"/> No
56b. 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 privacy or publicity rights	<input type="checkbox"/> 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?			<input type="checkbox"/> Yes <input type="checkbox"/> No
58. Does the Applicant have a written policy for handling requests for retractions or corrections?			<input type="checkbox"/> Yes <input type="checkbox"/> 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?			<input type="checkbox"/> Yes <input type="checkbox"/> 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?			<input type="checkbox"/> Yes <input type="checkbox"/> 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?			<input type="checkbox"/> Yes <input type="checkbox"/> 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?			<input type="checkbox"/> Yes <input type="checkbox"/> No
60d. 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

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? (damage to, destruction, loss, theft, unauthorized disclosure)	<input type="checkbox"/> Yes <input type="checkbox"/> No
---	--



AXIS CYBER APPLICATION FOR SMALL BUSINESS

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? (wrongful collection, retention, sale, disposal, deletion, disclosure, use, control, processing, access or correction)	<input type="checkbox"/> Yes <input type="checkbox"/> No
63. 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)	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
67. Have any of these matters been reported to another insurer?	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> 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.



AXIS CYBER APPLICATION FOR SMALL BUSINESS

4. Any policy the Insurer issues will be issued in reliance upon these representations.
5. The Applicant will report to the Insurer immediately in writing any material change in the Applicant's activities, products and services.
6. The Applicant will report to the Insurer immediately in writing any material changes to the answers provided in this Application which occur or are discovered between the date of this Application and the effective date of the policy for which coverage is sought by submission this Application.
7. The Insurer reserves the right, upon receipt of any such notice, to modify or withdraw any proposal for insurance the Insurer has offered.

WARNING

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

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

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

Name _____

Name (signature) _____

Title _____

Date _____

TO BE COMPLETED BY PRODUCERS ONLY:

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

Producer Signature: _____



AXIS CYBER APPLICATION FOR SMALL BUSINESS

STATE FRAUD STATEMENT

ALABAMA

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

ARKANSAS

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

CALIFORNIA

For your protection, California law requires the following warning to appear on this form: Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

COLORADO

It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado division of insurance within the department of regulatory agencies.

DISTRICT OF COLUMBIA

Warning: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the Applicant.

FLORIDA

Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete or misleading information is guilty of a felony of the third degree.

KANSAS

A "fraudulent insurance act" means an act committed by any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.



AXIS CYBER APPLICATION FOR SMALL BUSINESS

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 APPLICATION FOR SMALL BUSINESS

OREGON

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

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

- A. The misinformation is material to the content of the policy;
- B. We relied upon the misinformation; and
- C. The information was either:
 - 1. Material to the risk assumed by us; or
 - 2. Provided fraudulently.

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

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

PENNSYLVANIA

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

PUERTO RICO

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

RHODE ISLAND

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

TENNESSEE

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.



AXIS CYBER APPLICATION FOR SMALL BUSINESS

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.